日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

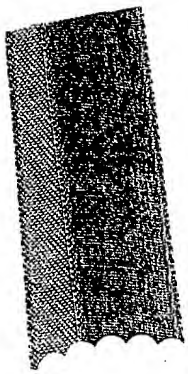
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

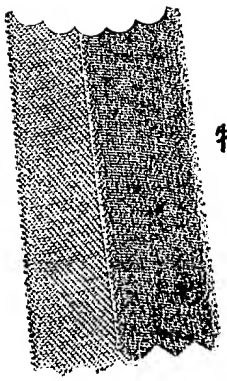
出願年月日
Date of Application: ２０００年　８月２４日

出願番号
Application Number: 特願２０００－２５３３０５

出願人
Applicant (s): ソニー株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT



２０００年１１月１０日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０９３９６５

【書類名】　特許願

【整理番号】　00003626

【提出日】　平成12年 8月24日

【あて先】　特許庁長官殿

【国際特許分類】　G06K 17/00

【発明の名称】　認証情報通信システムおよび認証情報通信方法、携帯情報処理装置、並びにプログラム提供媒体

【請求項の数】　48

【発明者】

【住所又は居所】　東京都品川区東五反田３丁目１４番１３号　株式会社ソニーコンピュータサイエンス研究所内

【氏名】　大場　晴夫

【発明者】

【住所又は居所】　東京都品川区東五反田３丁目１４番１３号　株式会社ソニーコンピュータサイエンス研究所内

【氏名】　戸塚　恵一

【発明者】

【住所又は居所】　東京都品川区東五反田３丁目１４番１３号　株式会社ソニーコンピュータサイエンス研究所内

【氏名】　暦本　純一

【発明者】

【住所又は居所】　東京都品川区東五反田３丁目１４番１３号　株式会社ソニーコンピュータサイエンス研究所内

【氏名】　松下　伸行

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　沼岡　千里

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100093241

【弁理士】

【氏名又は名称】　宮田　正昭

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【先の出願に基づく優先権主張】

【出願番号】　平成11年特許願第310517号

【出願日】　平成11年11月 1日

【手数料の表示】

【予納台帳番号】　062721

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　認証情報通信システムおよび認証情報通信方法、携帯情報処理装置、並びにプログラム提供媒体

【特許請求の範囲】

【請求項１】

人体を介した通信を行なう携帯情報処理装置とサービス提供装置とによって構成される認証情報通信システムにおいて、

前記携帯情報処理装置は、

人体と接触して人体を介した通信路を形成する接点Ａと、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段とを有し、

前記サービス提供装置は、

人体と接触して人体を介した通信路を形成する接点Ｂと、

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御手段と、

を有することを特徴とする認証情報通信システム。

【請求項２】

前記携帯情報処理装置は、

前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、

該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づく認証用データを生成する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項３】

前記サービス提供装置は、

前記携帯情報処理装置から、前記接点Ａ及び接点Ｂを介して転送される前記認

証用データに基づく認証処理を実行する認証手段を有し、

前記制御手段は、該認証手段の認証処理結果に基づいてサービスの実行を制御する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項４】

前記サービス提供装置は、

提供するサービスに応じたサービス識別子を保持するサービス識別子保持手段を有し、

前記携帯情報処理装置は、

前記可変データ記憶手段に、前記サービス識別子に対応して前記可変ユーザ識別データを格納する構成を有し、

前記サービス提供装置から前記接点Ｂおよび前記接点Ａを介して受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項５】

前記サービス提供装置は、

提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、

前記携帯情報処理装置は、

前記認証用ユーザ識別データ生成手段の生成した認証用ユーザ識別データを前記サービス提供装置から前記接点Ｂ、接点Ａを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項６】

前記認証情報通信システムは、さらに、

ユーザに対する認証処理を実行するユーザ管理手段を有し、

前記ユーザ管理手段は、

ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを有し、該登録テーブルに基づいて認証処理を実行する構成を有すること

を特徴とする請求項１に記載の認証情報通信システム。

【請求項７】

前記認証情報通信システムは、さらに、

ユーザに対する提供サービスを登録するサービス登録手段を有し、

該サービス登録手段は、

前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、

前記携帯情報処理装置は、

前記サービス登録手段において生成された認証用ユーザ識別データを前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする請求項１に記載の認証情報通信システム。

【請求項８】

前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする請求項１に記載の認証情報通信システム。

【請求項９】

サービス提供装置と人体を介して通信を実行する携帯情報処理装置において、

人体と接触して人体を介した通信路を形成する接点Ａと、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段と、

を有することを特徴とする携帯情報処理装置。

【請求項１０】

前記携帯情報処理装置は、

前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、

該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づ

く認証用データを生成する構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１１】

前記携帯情報処理装置は、

前記可変データ記憶手段に、前記可変ユーザ識別データをサービス識別子に対応させて格納する構成を有し、

前記サービス提供装置から受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１２】

前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１３】

前記接点Ａは、人体の装着部に沿った曲線形状を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１４】

前記携帯情報処理装置は、指、腕、首、脚部、足、頭部のいずれかに装着可能な構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１５】

前記携帯情報処理装置は、腕時計、ネックレス、指輪、ヘアバンド、ブレスレットのいずれかに内蔵された構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１６】

前記固定データ記憶部と前記可変データ記憶部は前記携帯情報処理装置に対して着脱可能な構成を有することを特徴とする請求項９に記載の携帯情報処理装置。

【請求項１７】

人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装

置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信方法において、

前記サービス提供装置から前記携帯情報処理装置に対して、前記接点Ｂおよび接点Ａを介してサービス識別データを転送するステップと、

前記携帯情報処理装置において、前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記携帯情報処理装置から前記サービス提供装置に対して、前記接点Ａおよび接点Ｂを介して前記認証用データを出力するステップと、

前記サービス提供装置において、前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とする認証情報通信方法。

【請求項１８】

前記認証用データ生成ステップは、

前記可変ユーザ識別データと、固定ユーザ識別データとを合成する合成ステップを含むことを特徴とする請求項１７に記載の認証情報通信方法。

【請求項１９】

前記サービス提供装置は、

前記携帯情報処理装置から、前記接点Ａ及び接点Ｂを介して転送される前記認証用データに基づく認証処理を実行する認証処理ステップを実行し、

前記制御ステップは、該認証処理ステップの認証処理結果に基づいてサービスの実行を制御することを特徴とする請求項１７に記載の認証情報通信方法。

【請求項２０】

前記認証情報通信方法において、

前記サービス提供装置は、

さらに、提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを有し、

前記携帯情報処理装置は、

前記認証用ユーザ識別データ生成ステップにおいて生成した認証用ユーザ識別データを前記サービス提供装置から前記接点Ｂ、接点Ａを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納することを特徴とする請求項１７に記載の認証情報通信方法。

【請求項２１】

前記認証情報通信方法において、さらに、

ユーザに対する認証処理を実行するユーザ管理ステップを有し、

前記ユーザ管理ステップは、

ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを生成するステップを含み、

前記認証処理は、該登録テーブルに基づいて実行することを特徴とする請求項１７に記載の認証情報通信方法。

【請求項２２】

前記認証情報通信方法において、さらに、

ユーザに対する提供サービスを登録するサービス登録ステップを有し、

該サービス登録ステップは、

前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを含み、

前記携帯情報処理装置は、前記サービス登録ステップにおいて生成された認証用ユーザ識別データを可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納するステップを有することを特徴とする請求項１７に記載の認証情報通信方法。

【請求項２３】

人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信システムにおいて、サービス提供装置で実行する処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納する記憶媒体であって、前記コンピュータ・ソフトウェアは、

前記サービス提供装置から前記接点Ｂを介して前記携帯情報処理装置に対して、サービス識別データを出力するステップと、

前記サービス識別データに対応する可変ユーザ識別データに基づいて前記携帯情報処理装置が生成した認証用データを前記接点Ｂを介して受信するステップと

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とする記憶媒体。

【請求項２４】

人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信システムにおいて、携帯情報処理装置で実行する処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に記憶する記憶媒体であって、前記コンピュータ・ソフトウェアは、

前記サービス提供装置から前記携帯情報処理装置に対して出力されるサービス識別データを前記接点Ａを介して受信するステップと、

前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記サービス提供装置に対して、前記接点Ａを介して前記認証用データを出力するステップと、

を有することを特徴とする記憶媒体。

【請求項２５】

人体を介したデータ転送を利用して認証手続を行う認証情報通信システムであって、

人体に搭載されて通信路を形成する第１の接点と、該第１の接点経由でデータ送信を行う第１のデータ送信部と、該第１の接点経由でデータ受信を行う第１のデータ受信部と、第１の制御部と、送信データ及び／又は受信データを格納可能

な第１のメモリとを備えた携帯装置と、

人体に接触して通信路を形成する第２の接点と、該第２の接点経由でデータ送信を行う第２のデータ送信部と、該第２の接点経由でデータ受信を行う第２のデータ受信部と、第２の制御部と、送信データ及び／又は受信データを格納可能な第２のメモリと、サービス提供を実現する駆動部とを備え、前記携帯装置に対して所定の情報処理サービスを提供する周辺装置と、

を具備することを特徴とする認証情報通信システム。

【請求項２６】

前記第１及び第２の制御部は、前記第１及び第２の接点及び人体経由の通信路が確立したことに応答して、前記第１のメモリ及び／又は前記第２のメモリに格納された認証情報を用いて認証手続を実行することを特徴とする請求項２５に記載の認証情報通信システム。

【請求項２７】

前記第１及び第２の制御部は、前記第１及び第２の接点及び人体経由の通信路が確立したことに応答して、一時的に発行するチャレンジ・キー並びに前記第１のメモリ及び／又は前記第２のメモリに格納された認証情報を用いてゼロ知識証明に基づく認証手続を実行することを特徴とする請求項２５に記載の認証情報通信システム。

【請求項２８】

前記第１の制御部は、前記周辺装置側からのデータ送信を待つ待機期間では前記第１のデータ受信部の電源を投入する一方で前記第１のデータ送信部の電源を遮断することを特徴とする請求項２５に記載の認証情報通信システム。

【請求項２９】

前記第１の制御部は、前記周辺装置に対してデータ送信を行う送信期間では前記第１のデータ送信部の電源を投入する一方で前記第１のデータ受信部の電源を遮断することを特徴とする請求項２５に記載の認証情報通信システム。

【請求項３０】

前記第２の制御部は、前記携帯装置との認証処理が成功したことに応答して、前記駆動部を利用したサービスを提供することを特徴とする請求項２５に記載の

認証情報通信システム。

【請求項３１】

前記第２の制御部は、前記携帯装置との認証処理が成功したことに応答して、前記携帯装置の識別情報に基づくサービスを前記駆動部を利用して提供することを特徴とする請求項２５に記載の認証情報通信システム。

【請求項３２】

前記第２の制御部は、前記の識別情報に基づくサービスに応じて、前記携帯装置のユーザに対する課金処理又はその一部を実行することを特徴とする請求項３１に記載の認証情報通信システム。

【請求項３３】

前記の識別情報に基づくサービスは、前記携帯装置に対して所定の権限情報の送信することを含むことを特徴とする請求項３１に記載の認証情報通信システム。

【請求項３４】

前記の識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して所定の装置の使用許可を含むことを特徴とする請求項３１に記載の認証情報通信システム。

【請求項３５】

前記の識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して該ユーザの嗜好や操作履歴に適応した処理を提供することを含むことを特徴とする請求項３１に記載の認証情報通信システム。

【請求項３６】

前記の識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して該ユーザに固有の操作環境を提供することを含むことを特徴とする請求項３１に記載の認証情報通信システム。

【請求項３７】

人体に搭載されて通信路を形成する携帯装置と、人体に接触して通信路を形成する周辺装置間において人体経由で認証手続を行う認証情報通信方法であって、

前記周辺装置が、人体との接触に応答して、前記携帯装置に対する認証又は識

別情報の要求を人体経由で送信するステップと、

前記携帯装置が、人体経由で認証又は識別情報の要求を受信したことに応答して、認証又は識別情報を人体経由で返信するステップと、

前記周辺装置が、人体経由で受信した認証又は識別情報に基づいて、前記携帯装置を認証処理するステップと、

を具備することを特徴とする認証情報通信方法。

【請求項３８】

前記携帯装置が、人体経由で認証又は識別情報の要求を受信するまでの待機期間中に受信機能を付勢するとともに送信機能を減勢するステップをさらに含むことを特徴とする請求項３７に記載の認証情報通信方法。

【請求項３９】

前記携帯装置が、人体経由で認証又は識別情報を送信する期間中に送信機能を付勢するとともに受信機能を減勢するステップをさらに含むことを特徴とする請求項３７に記載の認証情報通信方法。

【請求項４０】

人体に搭載されて通信路を形成する携帯装置と、人体に接触して通信路を形成する周辺装置間において人体経由で認証手続を行う認証情報通信方法であって、

前記周辺装置が、人体との接触に応答して、一度限り使用するチャレンジ・キーを人体経由で前記携帯装置に送信するステップと、

前記携帯装置が、人体経由でチャレンジ・キーを受信したことに応答して、認証又は識別情報と該チャレンジ・キーの組に対して所定の演算処理を適用するとともに、該演算結果を人体経由で返信するステップと、

前記周辺装置が、人体経由で受信した該演算結果に基づいて、前記携帯装置を認証処理するステップと、

を具備することを特徴とする認証情報通信方法。

【請求項４１】

前記携帯装置が、人体経由でチャレンジ・キーを受信するまでの待機期間中に受信機能を付勢するとともに送信機能を減勢するステップをさらに含むことを特徴とする請求項４０に記載の認証情報通信方法。

【請求項４２】

前記携帯装置が、人体経由で該演算結果を送信する期間中に送信機能を付勢するとともに受信機能を減勢するステップをさらに含むことを特徴とする請求項４０に記載の認証情報通信方法。

【請求項４３】

前記周辺機器が、前記携帯装置との認証処理が成功したことに応答して、前記携帯装置の識別情報に基づくサービスを提供するステップをさらに含むことを特徴とする請求項３７又は４０のいずれかに記載の認証情報通信方法。

【請求項４４】

前記周辺機器が、前記携帯装置の識別情報に基づくサービスに応じて、前記携帯装置のユーザに対する課金処理又はその一部を実行するステップをさらに含むことを特徴とする請求項４３に記載の認証情報通信方法。

【請求項４５】

前記の識別情報に基づくサービスは、前記携帯装置に対して所定の権限情報の送信することを含むことを特徴とする請求項４３に記載の認証情報通信方法。

【請求項４６】

前記の識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して所定の装置の使用許可を含むことを特徴とする請求項４３に記載の認証情報通信方法。

【請求項４７】

前記の識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して該ユーザの嗜好や操作履歴に適応した処理を提供することを含むことを特徴とする請求項４３に記載の認証情報通信方法。

【請求項４８】

前記の識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して該ユーザに固有の操作環境を提供することを含むことを特徴とする請求項４３に記載の認証情報通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、認証情報通信システムおよび認証情報通信方法、携帯情報処理装置、並びにプログラム提供媒体に関する。

【０００２】

さらに詳細には、外部機器に設けた電極である接点に人体の一部、例えば手が接触することによって、人体に装着したやはり電極としての接点を設けた携帯機器とのデータ通信を可能とし、個人認証に必要なデータを人体を介して転送して個人認証処理、および外部機器との情報交換を可能にした個人認証情報通信システムおよび個人認証情報通信方法に関する構成を開示するものである。

【０００３】

本発明に適用される携帯機器は、例えば時計や指輪のように曲線状の形状を有する取付具部を有し、人が通常身に付ける小型の物品において実現され、これらの装身具に個人認証のためのデータを記憶する構成としたものである。

【０００４】

【従来の技術】

昨今、情報処理や情報通信などのコンピューティング技術が飛躍的に向上し、コンピュータ・システムが広汎に普及してきている。さらに、コンピュータ同士を相互接続するネットワーク・コンピューティング技術に対する要望も高まってきている。ネットワーク上では、各コンピュータのユーザ同士で、コンピュータ資源の共有や、情報の共有・流通・配布・交換などの協働的作業を円滑に行うことができる。

【０００５】

コンピュータ同士を相互接続するネットワークの形態は様々である。例えば、企業内など局所に敷設されたＬＡＮ（Local Area Network）や、ＬＡＮ同士を専用線などで相互接続して構成されるＷＡＮ（Wide Area Network）、さらには、ネットワーク同士の相互接続を繰り返し行った結果として文字通り世界規模のネットワークへ成長を遂げた「インターネット」（The Internet）など様々である。

【０００６】

コンピュータのネットワーク接続率は既に高く、大学など各種研究機関、企業のオフィス、一般家庭などに深く浸透している。最近では、コンピュータ・ネットワークは、単なる情報配信の手段としてのみならず、商品売買を始めとして様々な商取引の手段として利用されている。いわゆる「ネット販売」又は「オンライン・ショッピング」と呼ばれる商取引である。

【０００７】

ネットワーク経由での商取引は、売主は、Ｗｅｂページの形式で商品情報を掲示して消費者からの反応（問合せや購入申込みなどの行為）を待機すればよく、店舗のショー・ケースなどの物理的な手段を省略して低コスト化を図ることができる。これは、一般の商品売買に限らず、リース・レンタルやその他の業務サービス全般にも同様に該当する。

【０００８】

また、ネットワークを利用した商取引の場合には、カタログに相当するデータ・コンテンツを特定のＷｅｂサイト上にアップロードしておくだけで、世界中に瞬間的に商品情報やサービス情報を配信することができる。すなわち、情報の即時性があり、商取引に関する契約を円滑且つ迅速に成立させることができる。また、ネットワーク配信によれば、商品販売に要するイニシャル・コストが低いので、取引単位を細分化して、一般消費者毎に区々な要望や各場所に散在する小規模な要望に関しても、逐次的に対応した取引を成立させることができる。

【０００９】

インターネット上での電子商取引や、音楽データその他のコンテンツのオンライン販売、あるいは売主やサービス提供者と消費者とが互いに離れた場所（又は、顔が見えない場所）に位置したまま取引が成立する様々な取引環境の普及に伴って、確実で簡単な個人認証技術に関する産業的な価値が高まってきている。何故ならば、一般の商取引と相違し、互いに見ることができない遠隔地のユーザを相手にしなければならず、「なりすまし」の危険が高いからである。

【００１０】

例えば、ユーザが自分の手もとにある情報機器を介して電子商取引やオンライン販売を行うような状況下では、購入手続のための入力操作以外に、自分自身で

あることを証明する認証手続を行わなければならない。購入手続と認証手続を別個に行っていたのでは、ユーザにとって操作が煩わしくなる。情報機器上で入力操作中に、ユーザの認証を並行して行うことができれば、以下のような便利な利用方法が可能になる。

【００１１】

（１）他人のコンピュータや携帯電話等を使っても取引をしても、機器の所有者ではなく、機器を操作している人の口座に課金することができる。

（２）自動販売機、公衆電話、キオスク端末など、不特定多数が扱う機器でも、操作した人に対して課金することができる。

（３）権利又は権限のある人が触るとロックが解除される（あるいは権限のないものが触るとロックされ又はロックが解除されない）ドア・ノブやドロワを作成することができる。

（４）権利又は権限のある人がハンドルに触れていないと、エンジンが始動しない自動車を実現することができる。

（５）テレビ受像機やＷｅｂブラウザのリモコンに、「その人がよく見る番組（又はよく閲覧するＷｅｂページ）」に切り替わるボタンを取り付けたりして、特定ユーザの嗜好や操作履歴に適応した処理を行うことができる。

（６）マウスに触れると、そのユーザの操作環境に自動的に切り替わるコンピュータ（又はそのユーザ・インターフェース）を実現することができる。例えば、マウスを持っているユーザが所有するファイルにアクセスするようにすることができる。

（７）テレビ・ゲームのゲーム・パッドやコントローラに触れると、その人向けに設定が切り替わる（例えば、既にクリアしたステージ、ゲームの履歴情報や、難易度設定など）。

（８）ペット・ロボットに触れると、そのロボットの所有者（又は正当なユーザ）か否かを認証し、その認証結果に基づく挙動を実行する。

【００１２】

従来、ユーザ認証を行うために、以下のような方法が行われていた。

【００１３】

（Ａ）ユーザにパスワードを入力させる方法

（Ｂ）指紋や網膜など、生体情報をキーとして使用する方法

（Ｃ）非接触型カードを利用する方法

【００１４】

（Ａ）による方法は、ユーザに煩雑な操作を要求することになる。また、パスワードを盗まれると、本人でなくても認証を受けることが可能になってしまい、確実性に欠ける。また、ある端末上で打ち込んだパスワードをネットワーク経由で伝送するような場合、伝送途上でパスワードが盗まれる危険性がある。これを回避するために、システムが提示するキーに対してユーザのパスワードを演算した結果をパスワードとして打ち込むＳ／ＫＥＹ方式が利用されているが、ユーザにはさらに煩雑な操作を要求することになる。

【００１５】

また、（Ｂ）による方法は、認証の際に、身体の特定の部位をセンサが認識できるように操作しなければならない。例えば、認証用の生体情報として網膜を使用する場合には、ユーザは自分の眼をセンサに向けなければならない。このような動作はユーザに身体的な不快感を与えるものである。また、現在の認識技術ではユーザを完全に特定することはできず、確実性に欠ける。

【００１６】

また、（Ｃ）による非接触カードなどを利用して個人認証を行い、認証の可否に基づいて外部装置を制御するシステムは既に広く知られている（例えば、特開平１１－１６１７６３号公報など）。非接触型カードは、定期券、プリペイド・カード等の接触型カードに変わるシステムとして今後有効な手法として期待される構成の１つである。例えば、ワイヤレス・タグのような識別情報や認証情報を電子的に取り出すことができるデバイスをキーとして用いることで実現することができる。

【００１７】

しかしながら、非接触型カードを使用するユーザは、カードによる認証を受ける際に、カードを自ら手に取り、例えばセンサ等の情報読み取り装置にカードを近づけて読み取り処理を実行させる必要がある。これらの一連の操作や処理には

時間を要するとともに、ユーザに煩わしい操作を強いるという欠点がある。例えば、入場ゲート、改札を通過するときなどの限られた時間内に一連の処理を次々と実行させなければならない場合、個人認証のためのカード読み取り、読み取りデータに基づく認証処理、認証処理に基づく改札ゲートの開閉動作を複数のユーザに対して次々と実行する必要がある。１人あたりの処理時間の増加は多人数の処理においてさらに大きな処理時間の増加をもたらし、実用化を困難にする原因となっている。この意味で非接触型カードは従来の接触型カードに比較して、すべての面で特に優れているとは言い難い。

【００１８】

さらに、非接触型カード又はカード型以外の認証用携帯機器を使用するユーザは、自分が取り出した、又は身に付けたカード等の認証機器を認証装置あるいは処理装置に近づけたり、あるいは近くを通り過ぎる等、極めて曖昧な処理を実行することが要求される。このような処理操作は、認証装置又は処理装置に直接触れるという確実な処理を伴わないので、実際にデータの読み取りに成功しているのか、あるいは個人認証処理が実行されているのか実感が得られず、処理の開始タイミング等が全くユーザには感覚的に判別することができない。したがって、処理が遂行されているか否かの判定が曖昧になってしまい、結果として、所定時間後に例えばゲートが開かないといったエラーが生じ、このエラーが生じるまでは、読み取り処理の失敗、または認証されなかったという結果が得られないという問題がある。

【００１９】

例えば、個人認証を行なおうとするユーザが、認証システムを構成する装置に形成された接点に対して人体の一部、例えば指や手のひら等を接触させることで人体を介して個人認証用データ転送を行なうことで、ユーザの個人認証処理の開始をユーザ自身が認識することを可能にするとともに、個人認証処理システムの使い勝手を改善することができる。また、ユーザに対して認証処理及び認証処理に基づく各種処理の実行が開始されたことの達成感という形態でフィードバックを与えることができる。

【００２０】

人体を介してデータ転送を行なうシステムに関しては、既に幾つか提案されている。

【００２１】

例えば、本出願人に既に譲渡されている特開平７－１７０２１５号公報や、米国特許第５，９１４，７０１号明細書には、電極を有する２つの互いに独立なシステムにおいて、そのままでは互いに通信するには不充分な程度の微弱電波をシステム間で発信し、そのシステム間に人体が介在することにより、人体を媒介としてシステム間のデータ転送を実行する構成が開示されている。

【００２２】

例えば特開平７－１７０２１５号公報に記載の信号伝送方式では、送信装置と受信装置間で身体（両手）で触れることによって、信号伝送が行われる。オーディオ／ビデオ信号等を導電性部材と人体を介して転送し、ディスプレイ、スピーカを備えた受信端末に出力する構成が記載されている。

【００２３】

また、米国特許第５，９１４，７０１号明細書には、身体内を通過する外部からの電流を検知し信号処理する非接触システムについて開示されている。

【００２４】

また、米国特許第５，７９６，８２７号明細書では、人体を介したデータ転送を使用したシステムについて開示されている。同システムでは、さらに暗号化したデータを送受する手段を加えることによって、クレジット・カードあるいはキャッシュ・カードなどに応用することができる。より具体的には、送信機から受信機に対する符号化データの転送を、人体を伝送媒体として実行し、受信機に接続された認証処理装置が人体を介して送られた符号化データを処理して認証を行なう構成である。

【００２５】

米国特許第５，７９６，８２７号には、人体を介するデータ転送を実行するための電極をユーザが日常身に付ける物品に組み込み可能とした構成が開示されている。ユーザが日常身に付ける物品の例として、腕時計、衣服、又は靴が記載されている。このような日常的に体に接触している物品、いわゆる装身具に電極を

組み込むことにより、ユーザが専用の電極構成体を新たに装着することを不要としている。

【００２６】

しかしながら、サービスの種類が多様化してきている昨今、認証処理を行なった後に実行すべき処理の態様は、ユーザによって、また場所や時間によって異なるものとすることが好ましい場合が多い。ユーザを認証処理によって識別して一律に認証の可否に応じた処理を実行することは、提供されるサービスの内容が固定的になり好ましくない。例えば、情報提供サービスを実行するサービス提供端末において、ＢＧＭ提供を受けようとすると、ユーザＡは、クラシックが好みであり、ユーザＢはロックが好みである場合、単なる認証処理に基づいて、同一の音楽配信をすると好みと無関係な音楽情報が配信される。あるいは、サービス提供端末が遊園地のゲートの開閉処理を制御する端末である場合、ユーザ毎にゲート開閉の有効時間、有効場所を設定することが望ましい。

【００２７】

勿論、ユーザ毎に提供サービスを設定するテーブルを設け、ユーザＩＤに基づいて提供サービスを決定し、決定したサービスを実行することも可能である。しかしながら、これらのデータ処理、すなわち情報提供端末からの中央処理装置へのデータ転送、データ処理装置におけるデータ処理、処理態様決定、さらに情報提供装置へのデータ転送等に時間を要し、次々に異なるユーザに対する処理を実行しなければならない環境等においては、処理時間の遅延が蓄積してしまうことになる。

【００２８】

また、上述したいずれのユーザ認証方法においても、ユーザはある程度の操作手順の習得が必要である。言い換えれば、「携帯電話を持つ」、「ドア・ノブに手が触れる」、「マウスをつかむ」といった単純な（又は通常の）操作に連動して認証を受けることはできない。さらに言えば、複雑な操作を要求せずに、認証通信の秘匿性、安全性を確保することもできない。

【００２９】

【発明が解決しようとする課題】

本発明は、上述したような課題を鑑みたものであり、ユーザ毎、サービス毎に異なる態様での処理を即座に実行可能にするように、各サービス毎に独立であり、かつ各ユーザ毎にユニークである認証用データを作成し、これをユーザの携帯機器に格納し、サービスの要求時にこの認証用データを出力できるようにすることを目的とする。

【００３０】

また、本発明は、非接触型カードが持つ利便性を損なうことなく、ユーザがサービス提供端末の接点に触れることによってユーザに処理の達成感を与えることができるように、人体を介して通信を行う携帯情報処理装置の接点を人体に接触した状態で装着するため、曲線状の接点部を持つ構成とすることを目的とする。

【００３１】

また、本発明は、接触型カード、非接触型カードと同様に個人認証を実行して各種の処理を実行させるシステムおよび方法において、個人認証を行なおうとするユーザが認証システムを構成する装置に形成された接点に対して人体の一部、例えば指や手のひら等を接触させることで人体を介して個人認証用データ転送を行ない、ユーザの個人認証処理の開始をユーザ自身が認識することを可能とし、個人認証処理システムの使い勝手を改善するとともに、ユーザに対して認証処理及び認証処理に基づく各種処理の実行が開始されたことの達成感を与えることができる個人認証情報通信システムおよび個人認証情報通信方法を提供することを目的とする。

【００３２】

また、本発明は、「携帯電話を持つ」、「ドア・ノブに手が触れる」、「マウスをつかむ」といった単純な（又は通常の）ユーザ操作に連動してユーザ認証を行うことができる認証システム及び認証方法を提供することを目的とする。

【００３３】

また、本発明は、ユーザに対して複雑な操作を要求することなく、認証通信の秘匿性や安全性を確保することを目的とする。

【００３４】

【課題を解決するための手段及び作用】

本発明は、上記課題を参酌してなされたものであり、その第１の側面は、人体を介した通信を行なう携帯情報処理装置とサービス提供装置とによって構成される認証情報通信システムにおいて、

前記携帯情報処理装置は、

人体と接触して人体を介した通信路を形成する接点Ａと、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段とを有し、

前記サービス提供装置は、

人体と接触して人体を介した通信路を形成する接点Ｂと、

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御手段とを有することを特徴とする認証情報通信システムである。

【００３５】

さらに、本発明の認証情報通信システムにおいて、前記携帯情報処理装置は、前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づく認証用データを生成する構成を有することを特徴とする。

【００３６】

さらに、本発明の認証情報通信システムにおいて、前記サービス提供装置は、前記携帯情報処理装置から、前記接点Ａ及び接点Ｂを介して転送される前記認証用データに基づく認証処理を実行する認証手段を有し、前記制御手段は、該認証手段の認証処理結果に基づいてサービスの実行を制御する構成を有することを特徴とする。

【００３７】

さらに、本発明の認証情報通信システムにおいて、前記サービス提供装置は、提供するサービスに応じたサービス識別子を保持するサービス識別子保持手段を

有し、前記携帯情報処理装置は、前記可変データ記憶手段に、前記サービス識別子に対応して前記可変ユーザ識別データを格納する構成を有し、前記サービス提供装置から前記接点Ｂおよび前記接点Ａを介して受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする。

【００３８】

さらに、本発明の認証情報通信システムにおいて、前記サービス提供装置は、提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、前記携帯情報処理装置は、前記認証用ユーザ識別データ生成手段の生成した認証用ユーザ識別データを前記サービス提供装置から前記接点Ｂ、接点Ａを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする。

【００３９】

さらに、本発明の認証情報通信システムは、ユーザに対する認証処理を実行するユーザ管理手段を有し、前記ユーザ管理手段は、ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを有し、該登録テーブルに基づいて認証処理を実行する構成を有することを特徴とする。

【００４０】

さらに、本発明の認証情報通信システムは、さらに、ユーザに対する提供サービスを登録するサービス登録手段を有し、該サービス登録手段は、前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成手段を有し、前記携帯情報処理装置は、前記サービス登録手段において生成された認証用ユーザ識別データを前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納する構成を有することを特徴とする。

【００４１】

さらに、本発明の認証情報通信システムにおいて、前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれること

を特徴とする。

【００４２】

また、本発明の第２の側面は、サービス提供装置と人体を介して通信を実行する携帯情報処理装置において、

人体と接触して人体を介した通信路を形成する接点Ａと、

ユーザ識別可能な固定ユーザ識別データを記憶する固定データ記憶手段と、

サービス提供装置の提供するサービスに対応する可変ユーザ識別データを保持する可変データ記憶手段と、

少なくとも前記可変ユーザ識別データに基づく認証用データを出力する出力手段と、

を有することを特徴とする携帯情報処理装置である。

【００４３】

さらに、本発明の携帯情報処理装置は、前記固定データ記憶手段に記憶された固定ユーザ識別データと、前記可変データ記憶手段に記憶された可変ユーザ識別データを合成する合成手段を有し、該合成手段は、前記固定ユーザ識別データと前記可変ユーザ識別データに基づく認証用データを生成する構成を有することを特徴とする。

【００４４】

さらに、本発明の携帯情報処理装置は、前記可変データ記憶手段に、前記可変ユーザ識別データをサービス識別子に対応させて格納する構成を有し、前記サービス提供装置から受信したサービス識別子に基づいて、前記可変データ記憶手段から対応する可変ユーザ識別データを抽出し、該抽出可変ユーザ識別データに基づく認証用データを出力する構成を有することを特徴とする。

【００４５】

さらに、本発明の携帯情報処理装置において、前記可変ユーザ識別データには、前記サービス提供装置の提供するサービスの態様設定情報が含まれることを特徴とする。

【００４６】

さらに、本発明の携帯情報処理装置において、前記接点Ａは、人体の装着部に

沿った曲線形状を有することを特徴とする。

【００４７】

さらに、本発明の携帯情報処理装置は、指、腕、首、脚部、足、頭部のいずれかに装着可能な構成を有することを特徴とする。

【００４８】

さらに、本発明の携帯情報処理装置は、腕時計、ネックレス、指輪、ヘアバンド、ブレスレットのいずれかに内蔵された構成を有することを特徴とする。

【００４９】

さらに、本発明の携帯情報処理装置において、前記固定データ記憶部と前記可変データ記憶部は前記携帯情報処理装置に対して着脱可能な構成を有することを特徴とする。

【００５０】

また、本発明の第３の側面は、人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信方法において、

前記サービス提供装置から前記携帯情報処理装置に対して、前記接点Ｂおよび接点Ａを介してサービス識別データを転送するステップと、

前記携帯情報処理装置において、前記サービス識別データに対応する可変ユーザ識別データを可変ユーザ識別データ格納手段から抽出するステップと、

抽出された前記可変ユーザ識別データに基づいて認証用データを生成する認証用データ生成ステップと、

前記携帯情報処理装置から前記サービス提供装置に対して、前記接点Ａおよび接点Ｂを介して前記認証用データを出力するステップと、

前記サービス提供装置において、前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とする認証情報通信方法である。

【００５１】

さらに、本発明の認証情報通信方法において、前記認証用データ生成ステップ

は、前記可変ユーザ識別データと、固定ユーザ識別データとを合成する合成ステップを含むことを特徴とする。

【００５２】

さらに、本発明の認証情報通信方法において、前記サービス提供装置は、前記携帯情報処理装置から、前記接点Ａ及び接点Ｂを介して転送される前記認証用データに基づく認証処理を実行する認証処理ステップを実行し、前記制御ステップは、該認証処理ステップの認証処理結果に基づいてサービスの実行を制御することを特徴とする。

【００５３】

さらに、本発明の認証情報通信方法において、前記サービス提供装置は、さらに、提供するサービスに応じた認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを有し、前記携帯情報処理装置は、前記認証用ユーザ識別データ生成ステップにおいて生成した認証用ユーザ識別データを前記サービス提供装置から前記接点Ｂ、接点Ａを介して受信し、前記可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納することを特徴とする。

【００５４】

さらに、本発明の認証情報通信方法において、前記認証情報通信方法において、

ユーザに対する認証処理を実行するユーザ管理ステップを有し、前記ユーザ管理ステップは、ユーザ登録状況および、登録ユーザごとのサービス利用状況を登録した登録テーブルを生成するステップを含み、前記認証処理は、該登録テーブルに基づいて実行することを特徴とする。

【００５５】

さらに、本発明の認証情報通信方法において、ユーザに対する提供サービスを登録するサービス登録ステップを有し、該サービス登録ステップは、前記サービス提供装置の提供するサービスに対応した認証用ユーザ識別データを生成する認証用ユーザ識別データ生成ステップを含み、前記携帯情報処理装置は、前記サービス登録ステップにおいて生成された認証用ユーザ識別データを可変ユーザ識別データ格納手段に可変ユーザ識別データとして格納するステップを有することを

特徴とする。

【００５６】

また、本発明の第４の側面は、人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信システムにおいて、サービス提供装置で実行する処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納する記憶媒体であって、前記コンピュータ・ソフトウェアは、

前記サービス提供装置から前記接点Ｂを介して前記携帯情報処理装置に対して、サービス識別データを出力するステップと、

前記サービス識別データに対応する可変ユーザ識別データに基づいて前記携帯情報処理装置が生成した認証用データを前記接点Ｂを介して受信するステップと、

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する制御ステップと、

を有することを特徴とする記憶媒体である。

【００５７】

また、本発明の第５の側面は、人体と接触して人体を介した通信路を形成する接点Ａを有する携帯情報処理装置と人体と接触して人体を介した通信路を形成する接点Ｂを有するサービス提供装置とによって実行される認証情報通信システムにおいて、サービス提供装置で実行する処理をコンピュータ・システム上で実行するように記述されたコンピュータ・ソフトウェアをコンピュータ可読形式で物理的に格納する記憶媒体であって、前記コンピュータ・ソフトウェアは、

前記サービス提供装置から前記接点Ｂを介して前記携帯情報処理装置に対して、サービス識別データを出力するステップと、

前記サービス識別データに対応する可変ユーザ識別データに基づいて前記携帯情報処理装置が生成した認証用データを前記接点Ｂを介して受信するステップと、

前記認証用データに基づく認証処理結果に基づいてサービスの実行を制御する

制御ステップと、

を有することを特徴とする記憶媒体である。

【００５８】

本発明の第４及び第５の各側面に係る記憶媒体は、例えば、様々なプログラム・コードを実行可能な汎用性のコンピュータ・システムに対して、コンピュータ・ソフトウェアをコンピュータ可読な形式で物理的に提供する媒体である。このような媒体は、例えば、ＣＤ（Compact Disc）やＦＤ（Floppy Disc）、ＭＯ（Magneto-Optical disc）などの着脱自在で可搬性の記憶媒体である。あるいは、ネットワーク（ネットワークは無線、有線の区別を問わない）などの伝送媒体などを経由してコンピュータ・ソフトウェアを特定のコンピュータ・システムにコンピュータ可読形式で提供することも技術的に可能である。

【００５９】

このような記憶媒体は、コンピュータ・システム上で所定のコンピュータ・ソフトウェアの機能を実現するための、コンピュータ・ソフトウェアと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、本発明の第４及び第５の各側面に係る記憶媒体を介して所定のコンピュータ・ソフトウェアをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の各側面に係る認証情報通信システムおよび認証情報通信方法と同様の作用効果を得ることができる。

【００６０】

また、本発明の第６の側面は、人体を介したデータ転送を利用して認証手続を行う認証情報通信システムであって、

人体に搭載されて通信路を形成する第１の接点と、該第１の接点経由でデータ送信を行う第１のデータ送信部と、該第１の接点経由でデータ受信を行う第１のデータ受信部と、第１の制御部と、送信データ及び／又は受信データを格納可能な第１のメモリとを備えた携帯装置と、

人体に接触して通信路を形成する第２の接点と、該第２の接点経由でデータ送信を行う第２のデータ送信部と、該第２の接点経由でデータ受信を行う第２のデータ受信部と、第２の制御部と、送信データ及び／又は受信データを格納可能な

第２のメモリと、サービス提供を実現する駆動部とを備え、前記携帯装置に対して所定の情報処理サービスを提供する周辺装置と、
を具備することを特徴とする認証情報通信システムである。

【００６１】

前記第１及び第２の制御部は、前記第１及び第２の接点及び人体経由の通信路が確立したことに応答して、前記第１のメモリ及び／又は前記第２のメモリに格納された認証情報を用いて認証手続を実行するようにしてもよい。

【００６２】

また、前記第１及び第２の制御部は、前記第１及び第２の接点及び人体経由の通信路が確立したことに応答して、一時的に発行するチャレンジ・キー並びに前記第１のメモリ及び／又は前記第２のメモリに格納された認証情報を用いてゼロ知識証明に基づく認証手続を実行するようにしてもよい。

【００６３】

また、前記第１の制御部は、前記周辺装置側からのデータ送信を待つ待機期間では前記第１のデータ受信部の電源を投入する一方で前記第１のデータ送信部の電源を遮断するようにしてもよいし、前記周辺装置に対してデータ送信を行う送信期間では前記第１のデータ送信部の電源を投入する一方で前記第１のデータ受信部の電源を遮断するようにしてもよい。

【００６４】

また、前記第２の制御部は、前記携帯装置との認証処理が成功したことに応答して、前記駆動部を利用したサービスを提供するようにしてもよい。ここで提供されるサービスは、例えば、前記携帯装置の識別情報に基づくサービスであってもよい。前記第２の制御部は、前記の識別情報に基づくサービスに応じて、前記携帯装置のユーザに対する課金処理又はその一部を実行するようにしてもよい。

【００６５】

ここで言う、識別情報に基づくサービスとは、例えば、前記携帯装置に対して所定の権限情報の送信することである。

【００６６】

あるいは、識別情報に基づくサービスは、前記携帯装置又はそのユーザに対し

て所定の装置の使用許可であってもよい。

【００６７】

あるいは、識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して該ユーザの嗜好や操作履歴に適応した処理を提供することであってもよい。

【００６８】

あるいは、識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して該ユーザに固有の操作環境を提供することであってもよい。

【００６９】

また、本発明の第７の側面は、人体に搭載されて通信路を形成する携帯装置と、人体に接触して通信路を形成する周辺装置間において人体経由で認証手続を行う認証情報通信方法であって、

前記周辺装置が、人体との接触に応答して、前記携帯装置に対する認証又は識別情報の要求を人体経由で送信するステップと、

前記携帯装置が、人体経由で認証又は識別情報の要求を受信したことに応答して、認証又は識別情報を人体経由で返信するステップと、

前記周辺装置が、人体経由で受信した認証又は識別情報に基づいて、前記携帯装置を認証処理するステップと、

を具備することを特徴とする認証情報通信方法である。

【００７０】

本発明の第６の側面に係る認証情報処理方法は、前記携帯装置が、人体経由で認証又は識別情報の要求を受信するまでの待機期間中に受信機能を付勢するとともに送信機能を減勢するステップをさらに含んでいてもよい。あるいは、前記携帯装置が、人体経由で認証又は識別情報を送信する期間中に送信機能を付勢するとともに受信機能を減勢するステップをさらに含んでいてもよい。

【００７１】

また、本発明の第７の側面は、人体に搭載されて通信路を形成する携帯装置と、人体に接触して通信路を形成する周辺装置間において人体経由で認証手続を行う認証情報通信方法であって、

前記周辺装置が、人体との接触に応答して、一度限り使用するチャレンジ・キ

ーを人体経由で前記携帯装置に送信するステップと、

前記携帯装置が、人体経由でチャレンジ・キーを受信したことに応答して、認証又は識別情報と該チャレンジ・キーの組に対して所定の演算処理を適用するとともに、該演算結果を人体経由で返信するステップと、

前記周辺装置が、人体経由で受信した該演算結果に基づいて、前記携帯装置を認証処理するステップと、

を具備することを特徴とする認証情報通信方法である。

【００７２】

本発明の第７の側面に係る認証情報処理方法は、前記携帯装置が、人体経由で認証又は識別情報の要求を受信するまでの待機期間中に受信機能を付勢するとともに送信機能を減勢するステップをさらに含んでいてもよい。あるいは、前記携帯装置が、人体経由で認証又は識別情報を送信する期間中に送信機能を付勢するとともに受信機能を減勢するステップをさらに含んでいてもよい。

【００７３】

また、前記周辺機器が、前記携帯装置との認証処理が成功したことに応答して、前記携帯装置の識別情報に基づくサービスを提供するステップをさらに含んでいてもよい。ここで提供されるサービスは、例えば、前記携帯装置の識別情報に基づくサービスであってもよい。このような場合、前記周辺機器が、前記携帯装置の識別情報に基づくサービスに応じて、前記携帯装置のユーザに対する課金処理又はその一部を実行するステップをさらに含んでいてもよい。

【００７４】

また、識別情報に基づくサービスは、例えば、前記携帯装置に対して所定の権限情報の送信することを含んでいてもよい。

【００７５】

あるいは、識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して所定の装置の使用許可を含んでいてもよい。

【００７６】

あるいは、識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して該ユーザの嗜好や操作履歴に適応した処理を提供することを含んでいてもよい

。

【００７７】

あるいは、識別情報に基づくサービスは、前記携帯装置又はそのユーザに対して該ユーザに固有の操作環境を提供することを含んでいてもよい。

【００７８】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００７９】

【発明の実施の形態】

以下、図面を参照しながら本発明の実施例を詳解する。

【００８０】

[実施例１]

本発明の認証情報通信システムの実施例１を構成する送受信装置全体の基本構成を示すブロック図として図１に示す。

【００８１】

図１に示すように、本実施例に係る認証情報通信システムは、携帯機器１０と、サービス端末２０を基本構成とし、携帯機器１０とサービス端末２０間でのデータ転送を、人体を介して実行するものである。このような人体経由での情報伝送のことを、本明細書中では「タッチネット」とも呼ぶ。

【００８２】

携帯機器１０は、ユーザ３０が保持または装着可能な機器として構成され、例えば腕時計や、ネックレス、ブレスレット、指輪、ベルト、靴等の装身具、またはカード等の部材によって構成することができ、接点１８は人体、すなわちユーザ３０と接触あるいは導通可能に極めて近接した状態に設定される。

【００８３】

サービス端末２０は、例えば、街頭あるいは店内などに配置されている音楽情報、映像情報、地図情報、その他、各種の情報提供あるいは商品販売用端末、キオスク端末、あるいは銀行に設置されたＡＴＭ（Automatic Teller Machine）端末、交通機関としての駅の改札ゲート、飛行機、電車その他の公共的乗り物の座

席、あるいは建築物の壁に埋設して設置されているような、様々なサービスを提供する装置である。ユーザ３０がサービス端末２０の接点２９に接触、すなわち指先で触れたり手のひらで触れたりすることにより、携帯機器１０とサービス端末２０の間で通信が可能になる。

【００８４】

人体を介する携帯機器１０とサービス端末２０間のデータ転送は、携帯機器１０に形成された接点１８と、サービス端末２０に形成された接点２９の両接点に同時に人体すなわちユーザ３０の一部が接触することによって実行される。

【００８５】

携帯機器１０は、例えば腕時計等の装身具であり、その接点１８は、基本的に人体への接触状態が常時確保され、あるいは導通可能に極めて近接した状態となっている。したがって、ユーザ３０がサービス端末２０の接点２９に触れることによって、人体を介する携帯機器１０とサービス端末２０間のデータ転送が実行可能となる。

【００８６】

携帯機器１０とサービス端末２０間のデータ転送は、携帯機器１０の通信部１５と、サービス端末２０の通信部２５との間で実行される。この人体を介した通信は、例えば、本出願人に既に譲渡されている特開平７－１７０２１５号公報に記載の構成を適用することができる。人体は、そのほとんどを塩分を含んだ水からなる導電性の容器と考えられるので、数ＭＨｚ帯では概ね導体となる（周知）。例えば、テスター等で両手間の直流抵抗を計測すると、手の状態に応じて５００ｋΩから２，３ＭΩの値を示す。

【００８７】

人体の交流における伝達特性を図２に示しておく。図２（ａ）は１ＭＨｚ～２０ＭＨｚの範囲で、図２（ｂ）は１ＭＨｚ～３０ＭＨｚの範囲で、それぞれスペクトラム・アナライザを用いて測定した人体の伝送特性（両手間）を示した特性図である。いずれも、トラッキング・ジェネレータと入力端子に同軸ケーブルを接続した場合の例である。なお、同軸ケーブルのグランドＧＮＤは相互に接続し、アンテナとならないようにした。図２（ａ）及び図２（ｂ）に示すように、１

ＭＨｚから２０ＭＨｚ程度の範囲における伝達特性は、概ね平坦で３０ｄＢ乃至４０ｄＢの減衰特性となる。

【００８８】

図２（ａ）及び図２（ｂ）に示す測定では、トラッキング・ジェネレータの出力インピーダンス、スペクトル・アナライザの入力インピーダンスともに７５Ωである。したがって、交流的にも両手間のインピーダンスが仮に１メガ・オームであったとすると、減衰量は－８０ｄＢにも達する筈である。ところが、実際には、減衰量は遥かに少なく、人体を介しての信号伝送の可能性を裏付けることが分かる。

【００８９】

データ送信側は、微小ダイポール・アンテナと考えられ、これが発生する電磁界の様子は充分解析されている。かかる解析結果によれば、人体が発生する電磁界は、微小ダイポール・アンテナが発生する電磁界となる。電磁界の強さはアンテナからの距離Ｒ、距離Ｒの２乗、距離Ｒの３乗に反比例する成分のベクトル和で表され、それぞれ、輻射電磁界、誘導電磁界、静電磁界と呼ばれる。なお、これらの関係式については、上述の特開平７－１７０２１５号公報に詳しく記載されている。

【００９０】

図３は電界強度についての図であり、図３（ａ）は、上述した各項の電界強度とアンテナからの距離との関係を示す特性図である。また、図３（ｂ）は、周波数ｆ＝２００ＭＨｚ、送信端子電圧＝１００ｄＢμＶ（７５Ω）の場合において、λ／２．２のダイポール・アンテナと３．４ｃｍφのループ・アンテナ、および８ｃｍφ，３．４ｃｍφのループ・アンテナの電界強度と距離とを示す図である。図３（ａ）および（ｂ）に示すように、上記輻射電磁界（１／Ｒ項）、誘導電磁界（１／（Ｒの２乗）項）、静電磁界（１／（Ｒの３乗）項）の強度は、λ／２πの距離において等しくなり、距離がこれ以下の場合には急激に増加する。ｆ＝１１ＭＨｚならば、この距離は約４．３ｍとなる。本発明の認証情報通信システムでは、静電磁界を主として使用した伝送方式を適用することが好ましいことが理解できよう。

【００９１】

また、電解強度は、電波障害すなわちＥＭＩ（ElectroMagnetic Inteference）に関する法規制による制限なく使用可能な範囲を選択することが好ましく、例えば、周波数３３２ＭＨｚ以下、電解強度５００μＶ／Ｍ以下とする。

【００９２】

上述のように静電磁界は距離Ｒの３乗で減衰する。例えば、距離が１ｍから３ｍになると、電界強度は１／２７（１／（３×３×３））に減衰する。したがって、データ送信手段からの距離の増加に伴って信号強度が極端に減衰するので、複数のユーザが同様の装置を使用している場合であっても他のユーザの信号をノイズとしてとらえる可能性は低くなる。例えば、同様の装置を持ったユーザが多数近接して存在するような作業環境下においても、静電磁界を主として使用した通信は良好な通信が可能になる。

【００９３】

なお、携帯機器１０に構成される接点１８は、広い面積を有することが望ましい。例えば、腕時計、ネックレス、指輪、ブレスレット、ベルト、靴等、曲線状に人体の指、腕、首等に巻き付け可能な構成として、人体の皮膚とより多くの面積で接触する構成とすることが好ましい。

【００９４】

携帯機器１０は、クレジット・カードの認証番号、ＡＴＭの暗証番号などのように、個人認証の目的で利用されるＩＤを記憶する認証用データ記憶部としての固定データ記憶部１６と可変データ記憶部１７を有している。固定データ記憶部１６には、ユーザ固有の固定ユーザ識別子が格納される。可変データ記憶部１７には、例えば、サービス端末のサービスに応じた識別子等、可変ユーザ識別子が格納される。これらの識別子の態様、および処理については後段で詳細に説明する。なお、固定データ記憶部１６と可変データ記憶部１７は、携帯機器１０に対して着脱・交換可能なメモリやその他のデバイスとして構成してもよい。

【００９５】

これらの固定ユーザ識別子、可変ユーザ識別子、あるいはこれらに基づく識別情報が携帯機器１０の通信部１５からサービス端末２０の通信部２５に送付され

ることによって、サービス端末２０のＣＰＵ（Central Processing Unit）２１において認証チェックがなされ、サービス端末２０の例えばＲＡＭ（Random Access Memory）２２などに記憶された情報にアクセスすることができる。サービス端末２０は、ＲＡＭ格納情報をサービス端末２０の通信部２５から携帯機器１０の通信部１５に送付し、データを受信した携帯機器１０は、ＲＡＭ１２等の記憶回路に受信データを蓄えることができる。なお、携帯機器１０のＲＯＭ（Read Only Memory）１３やサービス端末２０のＲＯＭ２３には、それぞれの装置の基本的な制御を行うＯＳ（Operating System）やデバイス・ドライバなどの基本ソフトウェアが記憶されており、電源を入れることによってＣＰＵによって読み出されそれぞれの装置を機能させることができる。

【００９６】

携帯機器１０の電源としては、図示していないが長寿命かつ小型の電源を使用することが望ましく、例えばリチウム電池セル（又は複数本の電池セルをパッケージ化したバッテリ・パック）を使用することができる。ＣＰＵ１１は、リチウム電池セルからの電源供給を受けてデータの読み出し、データ送信、データ受信、データ蓄積等の各種処理制御を実行する。

【００９７】

携帯機器１０とサービス端末２０との間での通信は、例えばサービス端末２０の接点２９に人体すなわちユーザ３０の一部が触れたことをサービス端末２０に設けた検知手段が検出し、この検出に応じて、サービス端末２０から後述するサービス識別子を通信部２５、接点２９、ユーザ３０を介して携帯機器１０に出力することにより開始することが可能である。

【００９８】

あるいは、サービス端末２０の通信部２５が連続的に、又は数秒間隔で、サービス識別子格納手段２８に格納されたサービス識別子データを出力する構成としてもよい。この構成における通信部２５のデータ出力間隔は、ユーザ３０がサービス端末２０の接点２９に指等を触れる数秒間に少なくとも1回は、送信信号がユーザを介してユーザの携帯する携帯端末１０の通信部１５によって受信されるような間隔とする。

【００９９】

あるいは、上記とは逆に、携帯機器１０の通信部１５が連続的に、又は数秒間隔で、固定データ記憶部１６、又は可変データ記憶部１７に記憶されたユーザＩＤなどの信号を送信する構成としてもよい。この場合も、ユーザ３０がサービス端末２０の接点２９に指等を触れる数秒間に少なくとも1回は、送信信号がサービス端末２０の通信部２５によって受信されるような間隔で発生する構成とする。

【０１００】

送信信号の種類は、後述するように認証処理においては、例えば、ユーザＩＤ、サービス識別子等の認証のために必要なデータである。

【０１０１】

認証処理後においては、サービス提供端末において、認証に基づく様々な処理が実行される。例えば、改札ゲートの開閉処理、ＡＴＭの入出金処理、あるいは音楽情報、画像情報、地図情報、商品情報等の各種コンテンツ情報の提供処理等である。

【０１０２】

なお、音楽情報、画像情報、地図情報、商品情報等の各種コンテンツ情報の提供を、人体を介して転送して携帯機器に蓄積したり、あるいは付属のディスプレイ等の出力手段で出力する構成としてもよい。なお、転送データ中に秘密情報を含む場合は、送信データをデータ送信側で暗号化して、受信側で暗号化データを復号処理する構成とすることが好ましい。この場合、データ送信側には、例えば、乱数発生手段、タイムスタンプ処理手段等、各種暗号化処理手段を構成する。一方、受信側には、受信した暗号化データを復号する復号手段を構成する。

【０１０３】

携帯機器１０とサービス端末２０に構成されるそれぞれの通信部は、ユーザ３０と各接点１８，２９との物理的接触により、信号を送受信することができる。受信信号は各通信部に構成された復調器により復調され、ＣＰＵ２１の制御下で、各端末内の回線、あるいは端末外のネットワークを通じて、各記憶手段、情報処理手段、あるいは認証処理手段等に転送される。

【０１０４】

なお、携帯機器１０は、データ送信やデータ処理が必要な場合にのみ、ＣＰＵに対する電源供給を実行するように構成（あるいは、ＣＰＵが稼動する）してもよい。例えば、サービス端末２０からの受信信号に基づいて電源供給を開始する構成（あるいは、ＣＰＵの動作を再開する構成）とすれば、携帯機器１０のバッテリ寿命を延ばすことができる。

【０１０５】

以下、図１に示す認証情報通信システムにおける認証処理、並びにデータ転送処理について、具体例を示しながら説明する。携帯端末１０を装着したユーザ３０がサービス端末２０に接点２９で接触したとする。ユーザ３０が初めてサービス端末２０に接触した場合には、認証のための登録処理がなされる。

【０１０６】

認証登録処理のために、サービス端末２０では認証用ユーザ識別子生成部２６において認証用のユーザ識別データ（可変ユーザ識別子）を生成し、このユーザ識別データ（可変ユーザ識別子）をサービス識別子２８とともに、通信部２５を経由して携帯端末１０の通信部１５に対して送信する。送信されたユーザ識別データ（可変ユーザ識別子）は、携帯端末１０の可変データ記憶部１７に記憶される。

【０１０７】

可変データ記憶部１７の構成及び合成部１４での処理について、図４を参照しながら説明する。可変データ記憶部１７は、例えば図４に示すようにテーブル構造をなしており、サービス端末２０から受信したサービス識別子（例えばサービスＩＤ：１０１）をキーとするレコードに対して、認証用ユーザ識別子（可変ユーザＩＤ：０００１００１１）を格納する構成となっている。

【０１０８】

携帯機器１０の合成部１４は、図４に示すようにサービス端末２０から受信した認証用ユーザ識別子（可変ユーザ識別子（ＩＤ）：０００１００１１）と、予め固定データ記憶部１６に格納されているユーザ固有の固定識別子（固定ユーザ識別子（ＩＤ）：１０１００００）との合成処理を実行する。

【０１０９】

合成部１４における合成処理により生成された識別子は、そのユーザ（固定ユーザＩＤ：１０１００００００によって特定される）にのみ有効であり、さらにそのサービス（例えばサービスＩＤ：１０１によって規定されるサービス）にのみ有効な識別子、すなわち特定サービスに有効なサービス固有のユーザ識別子である。

【０１１０】

携帯機器１０は、この合成部１４において生成された特定サービスに有効なサービス固有のユーザ識別子、例えば図４右上に記載のサービス：０１０用のユーザ識別子（ＩＤ）「１０１００００００／０００１００１１」を、サービス端末２０に対して送信する。携帯機器１０からサービス端末２０に対して人体を介して送信されるこのサービス固有のユーザ識別子は携帯機器１０の接点１８、ユーザ３０、サービス端末２０の接点２９を通じてサービス端末２０の通信部２５において受信される。

【０１１１】

サービス端末２０は、受信データを認証用データ記憶部２７に記憶する。認証用データ記憶部２７は、可変データ記憶部１７と同様の、例えばハッシュ・テーブル構造のような、認証用ユーザ識別子としての固定ユーザ識別子をキーとしたテーブル構成を有しており、受信したサービス固有のユーザ識別子をテーブルに記憶する。

【０１１２】

他方、ユーザ３０がサービス端末２０に接触したのが初めてでない場合には、サービス端末２０が保持するサービス識別子２８のデータ（例えば０１０）を受信した携帯端末１０は、受信サービス識別子に基づいて可変データ記憶部１７から受信したサービス識別子に対応する認証用ユーザ識別子（可変ユーザＩＤ）を取り出して、合成部１４において、固定データ記憶部１６に格納されているユーザ固有の固定識別子（固定ユーザＩＤ）との合成処理を実行してサービス固有のユーザ識別子を生成してサービス端末２０に送信する。

【０１１３】

この処理の具体例について、図４を参照しながら説明する。サービス端末２０の提供するサービス識別子が「０１０」であったとする。例えば、サービス端末２０がコンビニエンス・ストアなどの公共スペースに設置された情報提供端末であり、サービス識別子が「０１０」が商品割引券発行サービスであるとする。携帯端末１０（例えば腕時計に内蔵されている）を有するユーザは、コンビニエンス・ストアに設置されたサービス端末２０の接点２９に指、あるいは手のひらを触れる。サービス端末２０は、接点２９に設置されたセンサにより、指、あるいは手のひらの接触を検出し、ＣＰＵ２１の制御下でサービス識別子保持部２５からサービス識別子「０１０」を取り出して、これを通信部２５を介してユーザ３０に出力する。サービス識別子「０１０」は、ユーザ３０の人体を介して、ユーザの皮膚と接点１８を持つ腕時計型の携帯端末１０によって受信される。

【０１１４】

サービス識別子「０１０」を受信した携帯端末１０は、可変データ記憶部１７を検索して、サービス識別子「０１０」に相当する可変ユーザＩＤとして「０００１００１１」を取り出し、取り出した可変ユーザＩＤ「０００１００１１」を合成部１４に送る。合成部１４は、可変ユーザＩＤ「０００１００１１」と、固定データ記憶部１６に記憶されている固定ユーザＩＤ「１０１００００」とを合成し、「１０１０００００００１００１１」という特定サービスに有効なサービス固有のユーザ識別子データを得て、これを通信部１５、接点１８、ユーザ３０の人体、サービス端末２０の接点２９、を介してサービス端末２０の通信部２５に送信する。

【０１１５】

上述の処理を経て特定サービスに有効なサービス固有のユーザ識別子データを携帯端末１０から受信したサービス端末２０は、認証処理を行なう。この認証処理について図５を参照しながら説明する。

【０１１６】

サービス端末２０では、携帯端末１０から送信されるサービス固有のユーザ識別子データ、すなわち上述のデータ「１０１０００００００１００１１」を受信すると、認証部２４において、固定ユーザＩＤ「１０１００００」と、可変

ユーザＩＤ「００００１００１１」とに分離する処理を行なう。さらに、認証データ記憶部２７にアクセスして、これらの識別子が認証データ記憶部２７に登録済みのＩＤに対応するか否かの確認、すなわち認証処理を行う。正しくデータ照合がなされた場合、すなわち認証がされた場合には、サービス端末２０に規定されたサービス、すなわち上述のサービス識別子「０１０」に相当するサービス、例えば商品割引券発行サービスを実行する。サービス端末２０は、商品割引券発行手段と接続しているか、あるいはこれを内蔵しており、この商品割引券発行手段が認証処理に基づいて商品割引券発行処理が開始される。

【０１１７】

可変ユーザＩＤは、例えば、サービス端末２０において商品割引券発行が可能な期間を設定したデータとして構成することができる。この構成とした場合、可変ユーザＩＤを受信したサービス端末２０は、その可変ユーザＩＤから有効期間を判定して、有効期間内の場合にのみ正当なサービスを受けるユーザであると判定し、サービスを実行する。また、定期券等の場合は、期間、区間データも併せて可変ユーザＩＤ中に登録することで、携帯機器１０から受信した可変ユーザＩＤのみからその有効性を判定することが可能となる。

【０１１８】

サービス端末２０が提供するサービスは、例えば、入場ゲート、改札、建物の入口、研究室ドアの開閉処理であったり、画像、音声データ等の出力処理、ＡＴＭにおける入金、出金処理等、様々なサービスである。サービスが改札ゲートの開閉である場合は、上述の認証処理に基づいて、改札がオープンし、認証されたユーザのみが改札を通ることができる。この場合、サービス端末２０の接点２９は各改札ゲートに設置される。

【０１１９】

なお、サービス端末２０は、複数のサービス識別子を保持し、各々のサービス識別子に対応してサービス固有のユーザ識別子データを格納したテーブルを保持する構成とすることにより、各個人に対して異なるサービスを提供することが可能である。

【０１２０】

また、上述の例では、固定ユーザＩＤと可変ユーザＩＤとを単純に連結したデータを合成データとして生成し、これをサービス固有のユーザ識別データとする例を説明したが、サービス固有のユーザ識別データの生成は、上述した方法に限らず、固定ユーザＩＤと可変ユーザＩＤに基づいて予め定めた関数等により新たなデータ列を生成してサービス端末２０に送信し、サービス端末２０がこれを解読する構成としてもよい。これらの関数処理、解読処理は、例えば暗号化処理、復号処理の組合わせとしてもよい。また、可変ユーザＩＤのみをサービス端末２０に出力して、サービス端末２０が可変ユーザＩＤのみに基づいて認証処理を実行してユーザの識別及びサービスの実行可否を決定するように構成してもよい。サービス端末２０は、サービスに応じてユーザに可変ユーザＩＤを設定する構成であるので、可変ユーザＩＤのデータにユーザ個々の情報、提供サービスの情報、制限等、各種情報を含ませることが可能になる。

【０１２１】

サービス端末２０が情報提供を行なう端末である場合、認証処理を経て提供する情報は、音楽情報、画像情報など様々である。また、情報提供の形態も様々であり、サービス端末２０に設けたディスプレイ等の表示手段に表示してもよい。あるいは、携帯機器に付属して設けたディスプレイ等の出力手段に、上述の認証データと同様に人体を介してサービス端末２０から画像情報等の提供情報を転送して、ユーザに提供する構成としてもよい。なお、人体を介した画像、音声情報等の伝送態様については、本出願と同一出願人による先述した特開平７－１７０２１５号公報に詳細に説明されているので、参照されたい。

【０１２２】

携帯端末１０の例を図６に示している。図６（ａ）は、ブレスレット６０１に接点を設けて、内部に図１に示す携帯機器１０としての構成を内蔵した例である。また、図６（ｂ）は、ネックレス６０２に接点を設けて、その内部に図１に示す携帯機器１０としての構成を内蔵したものである。また、図６（ｃ）は、指輪６０３に接点を設けて、その内部に図１に示す携帯機器１０としての構成を内蔵したものである。また、図６（ｄ）は、腕時計６０４に接点を設けて、その内部に図１に示す携帯機器１０としての構成を内蔵したものである。ブレスレット６

０１、ネックレス６０２、指輪６０３、及び腕時計６０４の各々に設けられた接点は、それぞれ人体と接触する側、すなわち内周側に設けられおり、各接点を介して、ユーザである人体、さらにユーザの指、手のひら等、図１に示すサービス端末２０の接点２９に触れた人体の物理的接触点を介して携帯機器１０とサービス端末２０との間のデータ転送が可能になる。このように、携帯端末１０は、腕時計、ネックレス、指輪、ヘアバンド、ブレスレット等、指、腕、首、脚部、足、頭部のいずれかに装着可能な構成を有する。

【０１２３】

次に、図７～図９を用いて本発明の認証情報通信システムにおける認証処理フローについて説明する。図７は、図１に示す認証情報通信システムにおける携帯機器１０の処理手順をフローチャートの形式で示している。また、図８及び図９は、図１に示す認証情報通信システムにおけるサービス端末２０の異なる態様での処理手順を示したフローチャートである。

【０１２４】

まず、図７の携帯機器１０側の処理フローについて説明する。ステップ７０１はデータ受信のため、接点１８の電位上昇を確認するステップであり、データ受信に必要な電位を閾値として接点１８の電位を判定する。接点電位がデータ受信可能状態になると、ステップ７０２において、サービス端末２０からユーザ３０の人体を介して送られるサービスＩＤを受信する。

【０１２５】

サービスＩＤを受信した携帯端末１０は、ステップ７０３において、受信したサービスＩＤに対応する可変ユーザＩＤを可変データ記憶部１７から取り出し、さらに固定データ記憶部１６から固定ユーザＩＤを取り出して合成部１４において合成処理を行ない、認証用ＩＤを生成し、ステップ７０４において、生成した認証用ＩＤをサービス端末２０に対して人体を介して出力する。

【０１２６】

認証用ＩＤをサービス端末２０に出力した携帯端末１０は、ステップ７０５においてデータ受信側、すなわちサービス端末２０からの承認応答を待つ。承認応答を受信した場合は、サービス端末２０からのさらなる処理要求を待機（ステッ

プ７０６）する。そして、要求があった場合は、ステップ７０７において処理を実行する。

【０１２７】

この図７に示すフローは特定のサービス端末、例えば銀行のＡＴＭ等を想定した場合の処理フローである。図７のフローにおけるステップ７０５以降の処理は、サービス端末の態様によって異なるものとなる。サービス端末２０が銀行端末である場合、例えば、ステップ７０５の承認応答は、ステップ７０４での出力ＩＤに基づく認証がなされた後のディスプレイへの承認表示処理に相当し、ステップ７０６の処理要求は、例えば引き出し金額の指定要求であり、ステップ７０７の処理実行は、ユーザによる金額指定の処理等に対応する。

【０１２８】

また、サービス端末が改札ゲートであるとすると、ステップ７０４において、ユーザの携帯機器から認証用ＩＤの出力がなされると、サービス端末である改札ゲートに接続された端末は、認証の可否に基づいて改札ゲートの開閉を実行することになる。このように、図７の処理フローはサービス端末の提供する処理に応じて異なるものとなる。

【０１２９】

次に、サービス端末側での処理例について図８を参照しながら説明する。図８に示す例は、駅の改札のように、機器の動作を処理するだけのサービスの例である。

【０１３０】

ステップ８０１は、データ送信のため、接点２９の電位上昇を確認するステップであり、データ送信に必要な電位を閾値として接点２９の電位を判定する。接点電位がデータ送信可能状態になると、ステップ８０２において、サービス端末２０からユーザ３０の人体、接点２９を介して携帯機器１０に対してサービスＩＤを送信する。

【０１３１】

サービスＩＤを受信した携帯機器１０は、受信したサービスＩＤに対応する可変ユーザＩＤを可変データ記憶部１７から取り出し、さらに固定データ記憶部１

６から固定ユーザＩＤを取り出して合成部１４において合成処理を行ない、認証用ＩＤを生成し、生成した認証用ＩＤをサービス端末２０に対して出力する。サービス端末２０は、携帯機器１０からの認証用ＩＤを受信すると（ステップ８０３）、受信認証用ＩＤの認証処理を実行する。この処理は、図１における認証部２４が実行する（ステップ８０４）。

【０１３２】

認証部２４における認証の結果、認証用ＩＤの正当性が判定され（ステップ８０５）、正当であると判定されると、ステップ８０６においてサービス端末２０に設定されたサービスが実行される。

【０１３３】

一方、ステップ８０５における判定処理で、正当でないと判定されると、ステップ８０７に進み、サービスは中止され、処理が終了する。

【０１３４】

次に、サービス端末側での他の処理例について図９を参照しながら説明する。図９に示す例は、情報端末のように画像情報、音楽情報等、各種情報を提供するサービスの場合の処理例である。

【０１３５】

ステップ９０１は、データ送信のため、接点２９の電位上昇を確認するステップであり、データ送信に必要な電位を閾値として接点２９の電位を判定する。接点電位がデータ送信可能状態になると、ステップ９０２において、サービス端末２０から接点２９、ユーザ３０の人体を介して携帯機器１０に対してサービスＩＤを送信する。

【０１３６】

サービスＩＤを受信した携帯機器１０は、受信したサービスＩＤに対応する可変ユーザＩＤを可変データ記憶部１７から取り出し、さらに固定データ記憶部１６から固定ユーザＩＤを取り出して合成部１４において合成処理を行ない、認証用ＩＤを生成し、生成した認証用ＩＤをサービス端末２０に対して出力する。サービス端末２０は、携帯機器１０からの認証用ＩＤを受信すると（ステップ９０３）、受信認証用ＩＤの認証処理を実行する（ステップ９０４）。この処理は、

図１における認証部２４が実行する。

【０１３７】

認証部２４における認証の結果、認証用ＩＤの正当性が判定され（ステップ９０５）、正当でないと判定されると、ステップ９０９においてサービスが中止され、処理を終了する。

【０１３８】

他方、ステップ９０５において認証用ＩＤが正当であると判定されると、ステップ９０６においてサービス端末２０に設定されたサービスに規定された処理要求を出力する。さらに、ステップ９０７において、処理要求に対する応答を待機し、応答があった場合は、ステップ９０８において処理を実行し、要求データの送信を行なう。

【０１３９】

上述した図８及び図９のサービス端末２０側の処理において、例えば、図８の処理フローは、ビルでのセキュリティチェック・サービスの例に相当する。この場合、ステップ８０６のサービスは、ビルのドアの開閉の制御になり、ステップ８０７のサービス中止はドアの開閉処理の中止を意味する。さらに、ステップ８０７のサービス中止に伴う処理として不当ＩＤを登録するとった処理を行う構成としてもよい。

【０１４０】

また、図８の処理フローは、交通システム精算サービスの例にも相当する。この場合、ステップ８０６のサービスは改札ゲートの開閉をコントロールするだけでなく、料金精算が必要な場合には、電子精算処理をも行う構成とすることができる。

【０１４１】

また、図８の処理フローは、携帯電話や、ディスプレイを有するその他の携帯端末の利用形態としても適用可能である。例えば、図１０（ａ）に示す携帯電話や、同図（ｂ）に示すＰＤＡ（Personal Digital Assistant）等のディスプレイ機器などを利用した処理が可能である。ここで、図１０（ａ）に示す携帯端末は、導電性の接点を具備することを特徴とするサービス端末であり、また、図１０

（ｂ）ディスプレイ端末は、導電性のあるジョグダイヤルを具備することを特徴とするサービス端末である。

【０１４２】

図１０（ａ）に示す携帯電話において、図８に示すサービス端末の処理を実行する場合、サービス端末としての携帯電話を複数人で使う利用形態において、ユーザの識別データを腕時計等の携帯機器から携帯電話にユーザの人体を介して転送し、認証用ＩＤの正当性が確認された場合のみ携帯電話の使用が可能となる構成が実現される。このような場合、図８に示すステップ８０６におけるサービスは、通話可能モードへの設定処理となる。なお、携帯電話のディスプレイ領域に認証用ＩＤに相当する電話番号リストを表示するようにしてもよい。また、図１０（ｂ）に示すように、サービス端末としてＰＤＡ等のディスプレイ機器を使用する場合には、オンライン・ショッピングなどを行うときに、認証用ＩＤをベースにして、サービス・プロバイダとの認証を行い決裁を行うシステムとしての利用することが考えられる。

【０１４３】

さらに、図９に示した処理フローを実行するサービス端末の例として、リモート機器制御機器を挙げることができる。例えば、病院内などのように、電波を発生するために携帯電話の使用が制限されているような作業環境下で、ベッドから移動することができないような患者に対して、電話機器を利用することができるようなサービスを提供する端末が実現される。

【０１４４】

図９に示した処理フローを実行するサービス端末の例について、図１１を参照しながら説明する。

【０１４５】

患者４０が表示部を持つ腕時計タイプの携帯機器４１を身に付ける。患者４０が電話をかけたいときは、壁から吊り下げられたワイヤー状の接点４２に触れることにより、壁４３に埋め込まれたサービス端末４４、あるいは壁４３を通じて遠隔地に存在するサービス端末４４と通信を行う。

【０１４６】

患者４０がワイヤー状の接点４２を持つことにより、サービス端末４４からサービスＩＤが送信され（ステップ９０２）、これに応答して、携帯機器４１から認証用ＩＤが携帯機器４１に送られて、サービス端末４４において認証用ＩＤの正当性チェックが実行される（ステップ９０４）。

【０１４７】

認証処理で正当性が確認されると、処理要求、すなわち電話番号データの出力を患者４０に要求する（ステップ９０６）。電話番号データは、患者による音声出力、あるいは携帯機器４１に構成した電話番号データ入力キー等によって行なうことが可能な構成とし、これらの電話番号を受信したサービス端末４４は、電話を接続する処理を実行する（ステップ９０８）。

【０１４８】

図１１に示すような構成において、サービス端末４４には、モデムの機能が内蔵されている。サービス端末４４はさらに構内回線４５を通じてデジタル交換器４６と接続しており、この交換器４６から外部公衆回線網４７を通じて外部に電話をかけることが可能となる。

【０１４９】

なお、サービス端末４４が留守番電話の機能を有するようにすれば、患者がワイヤー状の接点４２を持つことにより、その情報を携帯機器４１に受信し、接点４２を離した後で、携帯機器４１の再生機能を使って、情報を再生することも可能である。

【０１５０】

[実施例２]

次に、本発明の第２の実施例について説明する。図１２には、第２の実施例を実現した認証情報通信システムの構成例を模式的に図解している。同図に示す認証情報通信システムは、ユーザ３０が装着した携帯機器１００と、サービス提供端末１１０と、サービス登録端末１２０と、認証課金等のユーザ管理を行うのためのクリアリングハウス１３０とで構成される。

【０１５１】

図１２に示す認証情報通信システムは、サービス提供端末１１０からのサービ

スを受けるユーザに対して、ユーザの認証処理のみならず、ユーザ毎に使用可能なサービスを設定するとともに、サービス利用状況を把握して、ユーザ単位の課金を可能としたシステムである。

【０１５２】

サービス提供端末１１０は、実際のサービスを提供する端末であり、例えば、音楽、画像情報等のコンテンツ情報の提供端末、あるいは遊園地の改札ゲート、駅の改札ゲート等、様々な場所に設置された様々なサービスを提供する端末などに相当する。なお、図１２には、サービス端末１１０が１つのみ記載されているが、サービス端末１１０はネットワーク１４０を介して複数台、必要な位置に存在していてもよい。例えば、サービス端末１１０が改札ゲートの開閉処理を実行する場合は、それぞれのゲート位置に配置されていてもよい。図１２では、図面の錯綜を防止するために、単一のサービス提供端末１１０の構成のみを記載していることを理解されたい。

【０１５３】

サービス提供端末１１０のＣＰＵ１１１は、ＲＡＭ１１３格納情報をサービス提供端末１１０の通信部２，１１５から携帯機器１００の通信部（図示しない）に接触又は非接触で送付し、データを受信した携帯機器１００は、携帯機器１００内のＲＡＭ等の記憶回路に受信データを蓄えることができる。なお、通信部１，１１４は、サービス登録端末１２０や、クリアリングハウス１３０との通信用である。さらに、サービス提供端末１１０のＲＯＭ１１２には、それぞれの装置の基本的な制御を行うＯＳやデバイス・ドライバなどの基本ソフトウェアが記憶されており、ＣＰＵ１１１によって読み出されそれぞれの装置を機能させることができる。

【０１５４】

サービス登録端末１２０は、ユーザ３０が、サービス提供端末１１０からのサービスを受けるために必要な登録を行なうための端末であり、例えばサービス提供端末１１０が駅の改札ゲートであれば、サービス登録端末１２０は定期券、切符等の販売を行なう駅に設置される。また、サービス提供端末１１０が遊園地の改札ゲートであればサービス登録端末１２０は入場券販売所等に設置される。ま

た、サービス登録端末１２０が音楽、画像情報等のコンテンツ情報の提供端末であれば、サービス登録端末１２０は、例えばコンビニエンス・ストアや駅のプラットフォームなどに設置されている情報提供端末、あるいはＡＴＭのような装置として構成することができる。

【０１５５】

サービス登録端末１２０のＣＰＵ１２１は、ＲＡＭ１２３格納情報をサービス登録端末１２０の通信部２，１２５から携帯機器１００の通信部（図示しない）に送付し、データを受信した携帯機器１００は、携帯機器１００内のＲＡＭ等の記憶回路に受信データを蓄えることができる。なお、通信部１，１２４は、サービス提供端末１１０や、クリアリングハウス１３０との通信用である。サービス登録端末１２０のＲＯＭ１２２には、それぞれの装置の基本的な制御を行うＯＳやデバイス・ドライバなどの基本ソフトウェアが記憶されており、ＣＰＵ１２１によって読み出されそれぞれの装置を機能させることができる。

【０１５６】

サービス登録端末１２０は、登録処理のための入出力機器、例えば、情報出力、入力用のディスプレイ、マイク、スピーカ等のユーザ入出力装置（いずれも図示しない）を備えている。携帯機器１００を装備したユーザ３０は、サービス登録端末１２０との通信においてもサービス登録端末１２０に設定された接点１２８を介した通信を実行する。携帯機器１００を装着したユーザ３０が、接点１２８においてサービス登録端末１２０に接触し、サービス登録端末１２０の接点１２８の電位が上昇し、通信可能な状態になると、サービス登録端末１２０は、まずユーザに対して、サービスの選択処理を実行することを要求する。

【０１５７】

サービス登録端末１２０のサービス選択部１２７は、ユーザに対してサービス登録端末１２０に構成されたディスプレイ、又はサービス登録端末１２０に接続されて配置されたディスプレイ（いずれも図示しない）に、図１３に示すようなメッセージ２０１を表示し、選択画面２０２中のサービス項目の中から１つを選択するように促す。

【０１５８】

ユーザ３０が、図１３に示すディスプレイの選択画面２０２上で、タッチ入力やキーボード入力、音声入力、その他の入力手段によりサービス項目の１つを選択すると、サービス登録端末１２０は、通信部２，１２５、接点１２８を介して、ユーザ３０に対して該選択されたサービスに対応するサービス識別子をユーザ３０の装着した携帯機器１００に送付する。

【０１５９】

サービス識別子を受信したユーザ３０の携帯機器１００は、上述の実施例１と同様に、可変データ記憶部１７（図１、図４を参照のこと）で可変ユーザＩＤを選択する。このとき、ユーザ３０が以前に一度も当該サービスを利用していなければ、この可変ユーザＩＤは初期化された値（例えば０などのデフォルト値）になっている。

【０１６０】

さらに、ユーザ３０の携帯機器１００の合成部１４（図１、図４を参照のこと）で固定データ記憶部１６内のデータ、すなわち予めユーザに対する固定値として設定されている固定ユーザＩＤと先述した可変データ記憶部１７に記憶されたサービスに対応する可変ユーザＩＤが合成されて生成されたサービス固有のユーザ識別子が、サービス登録端末１２０に送信され、通信部２，１２５において受信される。

【０１６１】

次に、サービス登録端末１２０は、通信部１，１２４を使ってクリアリングハウス１３０と通信を行うことにより、ユーザ３０の認証処理を行う。

【０１６２】

クリアリングハウス１３０は、図１２に示すように、サービス提供端末１１０やサービス登録端末１２０との通信を実行する通信部１，１３４と、基本的な制御を行うＯＳやデバイス・ドライバなどの基本ソフトウェアが記憶されたＲＯＭ１３２と、ＣＰＵ１３１によって実行されるプログラムのワークエリアと、入力されたデータなどを一時的に記憶するＲＡＭ１３３とを備え、ユーザ３０の認証処理を実行する装置である。ユーザ３０の認証処理は、インターネット、あるいはその他の通信回線１４０を介してクリアリングハウス１３０の通信部１，１３

４がユーザ３０の認証用データを受信し、受信したデータを認証部１３５に送り、ここでは前述の図４を参照しながら説明したと同様の処理手順を実行することで認証処理を行う。

【０１６３】

この実施例では、認証処理は、クリアリングハウス１３０の課金認証データ記憶部１３６に記憶された登録テーブルを用いて行なう。クリアリングハウス１３０の課金認証データ記憶部１３６は、例えば図１４に示されるようなデータ構造の登録テーブルを有しており、この登録テーブルにユーザ毎の最大使用度数、現在使用度数をセットする構成となっている。図１４に示す登録テーブル１４は一例であり、サービス態様に応じた項目、例えば個々のユーザに設定されたサービス使用期間、サービス使用時間、サービス使用地域、その他のサービスの詳細についての項目などのテーブル構成を、サービス提供端末１１０が提供するサービスに応じて設定する。

【０１６４】

ここで、図１４に示す登録テーブルを使用した場合には、ユーザごとの課金認証データ記憶部１３６の登録テーブルの状況として、以下の３つの態様が考えられる。

【０１６５】

（１）ユーザ３０は既に何らかのサービスを過去に使った履歴があり、固定ユーザＩＤが一致するレコードが課金認証データ記憶部１３６に存在しているが、今回の要求サービスに対応するレコードは存在しない。

（２）ユーザは、今回要求したサービスと同じサービスを過去に利用したことがあるので、対応する固定ＩＤレコードが存在する。

（３）ユーザは一度もサービスを利用したことがないので、ユーザのＩＤは登録されていない。

【０１６６】

上述の各態様において、（１）又は（３）の場合は、ユーザ３０から要求のあったサービスに対してユーザ登録が新たに必要となる。この場合、登録処理要求をサービス登録端末１２０に通知し、サービス登録端末１２０は、ユーザ３０か

ら要求のあったサービスに対するユーザ登録処理を実行する。より具体的には、ユーザ識別子生成部１２６において当該ユーザに対応するユーザ識別子（可変ユーザ識別子）を生成し、当該サービスのサービス識別子とともに、通信部２，１２５から接点１２８、ユーザ３０を介してユーザの携帯端末１００に送信する。これに対し、ユーザ３０の携帯端末１００では、受信したサービス識別子と可変ユーザ識別子との対を可変データ記憶部１７に対応させて記憶する（図４を参照のこと）。

【０１６７】

サービス識別子と、このサービス識別子に対応する可変ユーザ識別子とを、携帯機器１００の可変データ記憶部１７に登録した後は、ユーザは、携帯端末１００の合成部１４で、固定データ記憶部１７の固定ユーザ識別子と今回受信した可変ユーザ識別子とを合成し、サービス固有のユーザ識別子を生成して、これをサービス登録端末１２０に送付することによって、サービス登録端末１２０にユーザ登録処理の実行を依頼する。

【０１６８】

ユーザ登録依頼を受け取ったサービス登録端末１２０は、次にクリアリングハウス１３０に対して、受信したサービス固有のユーザ識別子を転送することにより、ユーザ登録を依頼する。このサービス固有のユーザ識別子データを受信したクリアリングハウス１３０は、自身の課金認証データ記憶部１３６に対して、当サービス固有のユーザ識別子に相当するレコードを作成し、最大使用度数を所定の数値にセットすると共に、現在使用度数を０として初期化する。

【０１６９】

上述の手続きを実行し、ユーザ登録が完了したユーザ３０は、サービス固有のユーザ識別子を携帯機器１００の可変データ記憶部１７に保持することになり、要求したサービスをサービス提供端末１１０経由で受けることができる。

【０１７０】

サービス提供を受けようとするユーザ３０は、サービス提供端末１１０の接点１１６に触れて、サービス提供端末１１０から、接点１１６及びユーザ３０の人体を介して携帯機器１００に対するサービス識別子の転送を受ける。携帯機器１

００は、これに応答して、登録した可変ユーザＩＤと固定ユーザＩＤを合成し、サービス固有のユーザ識別子を生成して、これをサービス提供端末１１０に転送する。

【０１７１】

さらに、このサービス固有のユーザ識別子が、クリアリングハウス１３０にネットワーク等を介して転送されて、認証処理、および課金認証データ記憶部１３６に格納された登録テーブルの使用度数の更新が行なわれる。認証処理は、前述の実施例１と同様の処理手順で実現される。ユーザ３０は、このような手続きを経て、使用度数に至るまでサービス提供端末１１０からのサービスを受けることができる。

【０１７２】

次に（２）の場合、すなわち、今回要求したサービスと同じサービスを過去に利用したことがあり、対応する固定ＩＤレコードが登録テーブルに存在する場合の処理について説明する。（２）の場合は、さらに、次の２つのケースが考えられる。

（２－１）まだ現在使用度数が最大使用度数を超えていない。

（２－２）すでに現在使用度数が最大使用度数を超えている。

【０１７３】

（２－１）の場合には、クリアリングハウス１３０は、サービス登録端末１２０に対して、「登録の必要がない」という意味のメッセージを送付する。サービス登録端末１２０は、このメッセージを受信することにより、ユーザ３０に対してその旨を通知して、処理全体を終了する。

【０１７４】

他方、（２－２）の場合には、クリアリングハウス１３０は、サービス登録端末１２０に対して、「更新の必要あり」という意味のメッセージを送付する。サービス登録端末１２０は、このメッセージを受信することにより、ユーザ３０に対してその旨を通知して、ユーザ３０に対して、更新するかどうかの問い合わせを行う。ユーザ３０が更新に同意する場合には、クリアリングハウス１３０に対して、更新処理を依頼する。

【０１７５】

クリアリングハウス３０における更新処理は、より具体的には、例えば、課金認証データ記憶部１３６の登録テーブルの対応するレコードの現在使用度数を０にセットする処理である。ユーザ３０が更新に対して同意しない場合には、さらにユーザ３０に対して、課金認証データ記憶部１３６の登録テーブルのレコードを削除するかどうかの問い合わせを行う。ユーザ３０がレコード削除に同意した場合には、クリアリングハウス３０に対して、当該レコードの削除を依頼し、クリアリングハウス３０は該当するレコードを課金認証データ記憶部１３６から削除する。ユーザ３０がレコード削除に同意しない場合には、サービス登録端末１２０はそのまま処理を終える。

【０１７６】

携帯端末１００を所持するユーザ３０が、サービス提供端末１１０に接点１１６で接触してサービスの提供を受ける場合の処理について説明する。サービス提供端末１１０にはサービスを提供するためのデータ入出力機器としての表示ディスプレイ１１８、マイク１１９が付属しており、サービス開始の際には、表示ディスプレイ１１８に、例えば図１５に示すような案内表示がなされる。表示ディスプレイにはサービス選択画面３０１が示される。

【０１７７】

ユーザ３０がサービス提供端末１１０の接点１１６に接触すると、サービス提供端末１１０は、サービス識別子記憶部１１７のデータを読出し、ユーザ３０の携帯端末１００に対してサービス識別子を通信部２，１１５、接点１１６、ユーザ３０の人体を介して送信する。

【０１７８】

ここで、図４を参照しながら、このサービス識別子受信後の処理を説明する。サービス識別子が「０１０」であったとする。この場合、携帯機器１００の可変データ記憶部１７においてサービス識別子「０１０」に相当するレコードには可変ユーザ識別子として「０００１００１１」が記憶されているので、これを、固定データ記憶部１６に記憶されている固定ユーザ識別子「１０１０００００」と合成部１４において合成処理を実行し、例えば、「１０１０００００００１０

０１１」というデータを生成する。

【０１７９】

このデータは、サービス固有のユーザ識別子であり、これをサービス提供端末１１０に送付する。当該データを受信したサービス提供端末１１０は、その後このデータをクリアリングハウス１３０に送付することによって、ユーザ認証・課金処理を依頼する。クリアリングハウス１３０では、サービス提供端末１１０から送信されたサービス固有のユーザ識別子データを受信すると、認証部１３５において、サービス固有のユーザ識別子に基づいて、固定ユーザ識別子「１０１０００００」と可変ユーザ識別子「０００１００１１」を分離生成する処理を実行した後、課金認証データ記憶部１３６にアクセスしてユーザが登録されているかどうかの認証を行う。

【０１８０】

その後、課金認証データ記憶部１３６にて図１４にあるような登録テーブルと照合して、認証が正しくなされた場合には、サービス提供端末１１０に対して「認証ＯＫ」のメッセージを送信すると同時に、課金認証データ記憶部の当該レコードの現在使用度数を１減少させる。クリアリングハウス１３０から「認証ＯＫ」のメッセージを受信したサービス提供端末１１０では、ユーザ３０に対するサービス提供が実行される。

【０１８１】

クリアリングハウス１３０において認証が失敗した場合には、サービス提供端末１１０に対して、付属するディスプレイ装置１１８等に「認証が失敗した」旨を通信するメッセージを表示することによって、処理を終了する。

【０１８２】

以上の例において、通信中のデータのセキュリティを考慮して、各構成要素の通信部１，１１４，通信部２，１１５，通信部１，１２４，通信部２，１２５，及び通信部１，１３４から送出されるデータを、暗号化装置（図示しない）によって暗号化して送出するようにし、各通信部において受信された後に復号化装置（図示しない）によって復号するようにしてもよい。

【０１８３】

上述した例では、サービス提供端末１１０がディスプレイを使用した情報提供を主に実行する構成である。但し、サービスの形態はこれに限定されない。ユーザに提供するサービスが駅、遊園地等の改札ゲートの開閉動作であってもよく、この場合、サービス提供端末１１０は、各駅、あるいは遊園地の複数の場所に設置された改札ゲートとして構成される。この場合、図１２に示したサービス提供端末１１０は、各ゲートに対応して配置される。ユーザ３０はサービス提供端末１１０の接点１１６に触れ、合成処理により生成されたサービス固有のユーザ識別子、この場合は、定期券の所定区間、所定期間に対応する改札開閉処理サービス固有のユーザ識別子をサービス提供端末１１０、クリアリングハウス１３０に転送し、認証処理、課金または清算処理を行ない、有効な認証処理がなされた場合のみ、改札ゲートをオープンさせる。

【０１８４】

認証処理は、既に説明したように、ユーザの装着した携帯機器１００とサービス提供端末とのユーザ３０を介した通信を実行して行われる。したがって、接点１１６は、各ゲートに設置された接点である。携帯機器１００を装着したユーザ３０が接点１１６を触れることで、認証処理が実行され、認証がなされた場合は、ゲートがオープンする。

【０１８５】

この場合、サービス登録端末１２０は、ユーザ３０がサービスを受けるために必要な登録を行なうための端末であり、定期券、切符等の販売を行なう駅、あるいは、入場券販売所等に設置される。

【０１８６】

サービス登録端末１２０での登録処理は、ユーザ３０がサービス登録端末１２０の接点１２８に触れることによって開始される。サービス登録端末１２０において、ユーザ３０は、特定のサービス、例えば、定期券の販売であれば、駅区間、有効期間の設定を行ない、これらの設定区間、期間のデータをクリアリングハウス１３０の課金認証データ記憶部１３６の登録テーブル中に登録し、登録テーブルを参照してユーザの認証処理を実行する。このように、サービス提供端末１１０の提供するサービスは各種可能であり、サービス単位、かつユーザ単位の認

証処理や管理が可能となる。

【０１８７】

なお、以上の説明では、基本的に認証を行う携帯機器についての例を述べたが、認証が不要な応用例、例えば、本携帯機器の認証機能をオフ、あるいはすべてのユーザを無条件に認証するとした設定とすることで、情報交換機器としても利用すること、すなわち外部情報入力システムとしての応用することが可能である。例えば、電車内での所定の位置、例えば、広告の一部、または吊革等に接点を構成することで、携帯機器を有するユーザがこれらの接点に接触することで、電車内の広告情報が携帯機器に入力されるようにすることができる。携帯機器中のメモリに情報を取り込んだり、あるいは携帯機器に付属するディスプレイ、スピーカを通じて情報を出力する構成としてもよい。

【０１８８】

さらに、図１６のように、腕時計型あるいはブレスレット型の携帯装置２０１、２０２を装着した２人のユーザが、携帯装置２０１、２０２をそれぞれ装着して握手を行なうことにより、携帯装置２０１と携帯装置２０２の間で、握手した人体を介するデータ転送を行なうことが可能である。また、携帯装置２０１と携帯装置２０２内に認証処理構成を内蔵させれば、認証された携帯機器を有するユーザ同士では、情報を転送することが可能であるが、認証されない相手に対しては、情報の転送が実行されない構成とすることができる。

【０１８９】

［実施例３］

本発明によれば、タッチネットすなわち人体経由での情報交換を利用して、ユーザが装着した携帯機器とユーザにサービス提供するサービス提供端末間での認証処理やサービス提供が、ユーザが触れるという物理的な実感を含んだフィードバックを伴って実現される、という点については、上記の実施例１並びに実施例２で説明した通りである。

【０１９０】

本発明の第３の実施例では、このタッチネットの技術を適用して、ユーザが触れた機器（例えば、携帯機器に対して接続される「周辺機器」）との間で個人認

証を行う方式について説明する。

【０１９１】

図１７には、この実施例に係る認証情報通信システムの機能構成を模式的に示している。同図に示すように、この認証情報通信システムは、ユーザが身体に装着して身体との接触が常に確保されているウェアラブル・デバイス３００と、ユーザの身体経由で接続可能な周辺デバイス３２０とで構成される。

【０１９２】

ウェアラブル・デバイスは、例えば腕時計や、ネックレス、ブレスレット、指輪、ベルト、靴等の装身具などに組み込む形式で実装され、タッチネット送信部３０１、タッチネット受信部３０２、ＣＰＵ３０３、メモリ３０４、並びに装置駆動用のバッテリ（図示しない）で構成される。

【０１９３】

メモリ３０４には、ＣＰＵ３０３において実行される装置駆動用のプログラム・コードの他に、利用者認証に使用される認証情報が格納されている。

【０１９４】

また、周辺デバイス３２０は、例えば、ウェアラブル・デバイスからの指示によって特定の情報処理や情報蓄積・読み出しなどの動作を行う補助的な外部機器類であり、タッチネット送信部３２１、タッチネット受信部３２２、ＣＰＵ３２３、メモリ３２４、並びに、ＣＰＵ３２３からの制御指示値に従って動作する駆動部３２５で構成される。

【０１９５】

メモリ３２４には、ＣＰＵ３２３において実行される装置駆動用のプログラム・コードの他に、ウェアラブル・デバイス３００との間での利用者認証に使用される認証情報が格納されている。

【０１９６】

ウェアラブル・デバイス３００を装着しているユーザが周辺デバイス３２０に触れるだけで、各デバイス３００，３２０間の認証手続が自動的に暗黙のうちに終了し、セキュアな状態で周辺デバイス３２０の使用が可能となる。したがって、周辺デバイス３２０を使用する際に、ログイン・パスワードのマニュアル入力

といったような煩雑な手続が不要となる。

【０１９７】

図１８には、ウェアラブル・デバイス３００と周辺デバイス３２０間で行われる認証手続をフローチャートの形式で示している。以下、このフローチャートに従ってデバイス３００，３２０間の認証手続について説明する。

【０１９８】

ウェアラブル・デバイス３００は、初期状態すなわち認証手続を開始しない状態では、タッチネット送信部３０１を電源オフにするとともにタッチネット受信部３０２を電源オンにして（ステップ１８１１）、受信のみ可能な状態（Receive Only）で待機する。

【０１９９】

待機状態においてタッチネット送信部３０１の電源をオフにする理由は、待機状態から動作を再開するのはＩＤ要求の受信しかあり得ず、送信部３０１の動作が不要だからである。また、送信部３０１の電源をオフにすることにより省電力化し、バッテリ駆動時間を延ばすことができる。

【０２００】

一方、周辺デバイス３２０は、ウェアラブル・デバイス３００を装着したユーザが電極に触れたことに応答して（ステップ１８０１）、ウェアラブル・デバイス３００に対してＩＤ要求を送信する（ステップ１８０２）。

【０２０１】

ＩＤ要求の送信は、周辺デバイス３２０側の電極、ユーザの身体、並びにウェアラブル・デバイス３００の電極を介した「タッチネット伝送」によって行われる。タッチネット伝送によれば、ユーザは、コマンド入力などの作業が不要であり、無意識のうちに認証手続を行うことができるので、ユーザに煩わさを感じさせない。

【０２０２】

ウェアラブル・デバイス３００側では、ＩＤ要求を受信すると、今度はタッチネット受信部３０２を電源オフにするとともにタッチネット送信部３０１を電源オンにする（ステップ１８１３）。そして、メモリ３０４からＩＤ情報を取り出

して、これを同様のタッチネット伝送により周辺デバイス３２０側に返す（ステップ１８１４）。

【０２０３】

タッチネット受信部３０２を電源オフにする理由は、ＩＤ送信時には受信部３０２の動作は不要となり、電源オフとすることにより省電力化してバッテリ駆動時間を延ばすためである。

【０２０４】

そして、ウェアラブル・デバイス３００は、ＩＤ送信を行った後は、ウェアラブル・デバイス３００は、再び待機状態すなわち受信待ち状態に遷移し、タッチネット送信部３０１を電源オフにするとともにタッチネット受信部３０２を電源オンにする（ステップ１８１１）。

【０２０５】

周辺デバイス３２０側では、タッチネット伝送によりＩＤ情報を受信すると（ステップ１８０３）、受信したＩＤ情報に対応する処理を実行する（１８０４）。そして、ステップ１８０１に復帰して、次にユーザが接触するまで待機する。

【０２０６】

ステップ１８０４におけるＩＤ情報に対応する処理とは、例えば、同じ周辺デバイス３２０であっても、ＩＤ情報すなわちユーザごとに提供するサービスを変えることを意味する。例えば、周辺デバイス３２０が情報蓄積装置である場合、特定の情報資源へのアクセスを許可しない、読み出しアクセスしか許可しない、フル・アクセスを許可するなど、ユーザごとに与える権限を変えるようにしてもよい。但し、ステップ１８０４で行う処理の詳細に関しては、後述に譲る。

【０２０７】

他方、周辺デバイス３２０がＩＤ情報の受信に失敗したときには（ステップ１８０３）、接触したユーザに対する処理を行うことなく、ステップ１８０１に復帰して、次にユーザが接触するまで待機する。

【０２０８】

また、ウェアラブル・デバイス３００と周辺デバイス３２０間の認証手続には、例えば「ゼロ知識証明」を用いることができる。ゼロ知識証明/*/とは、秘密

情報を知っていることを、秘密を明かさずに証明する方法のことであり、一般には、乱数と秘密情報から演算した結果を証明者と検証者間で交換して確率的に納得させることで実現される。例えば、ある通信路を偽って結合された２者Ｐ及びＶの間で、Ｐが秘密のパスワードＳを持っていることを、通信路にパスワードを流さずにＶが認証することができる。

【０２０９】

図１９には、ウェアラブル・デバイス３００と周辺デバイス３２０間で行われる、ゼロ知識証明を用いた認証手続をフローチャートの形式で示している。以下、このフローチャートに従ってデバイス３００，３２０間の認証手続について説明する。

【０２１０】

ウェアラブル・デバイス３００は、初期状態すなわち認証手続を開始しない状態では、タッチネット送信部３０１を電源オフにするとともにタッチネット受信部３０２を電源オンにして（ステップ１９１１）、受信のみ可能な状態（Receive Only）で待機する。

【０２１１】

タッチネット送信部３０１の電源をオフにする理由は、待機状態から動作を再開するのはＩＤ要求の受信しかあり得ず、送信部３０１の動作が不要だからである。また、送信部３０１の電源をオフにすることにより省電力化し、バッテリ駆動時間を延ばすことができる。

【０２１２】

一方、周辺デバイス３２０は、ウェアラブル・デバイス３００を装着したユーザが電極に触れたことに応答して（ステップ１９０１）、ウェアラブル・デバイス３００に対して１回限り使用するチャレンジ・キーを送信する（ステップ１９０２）。

【０２１３】

チャレンジ・キーの送信は、周辺デバイス３２０側の電極、ユーザの身体、ウェアラブル・デバイス３００の電極を介した「タッチネット伝送」によって行われる。

【０２１４】

ウェアラブル・デバイス３００側では、ＩＤ要求を受信すると、今度はタッチネット受信部３０２を電源オフにするとともにタッチネット送信部３０１を電源オンにする（ステップ１９１３）。そして、メモリ３０４からＩＤ情報を取り出して、ＩＤ情報とチャレンジ・キーの組に対して所定の演算を適用してＸを生成し（ステップ１９１４）、これをタッチネット伝送により周辺デバイス３２０側に返す（ステップ１９１５）。

【０２１５】

タッチネット受信部３０２を電源オフにする理由は、Ｘを送信時には受信部３０２の動作は不要となり、電源オフとすることにより省電力化してバッテリ駆動時間を延ばすためである。

【０２１６】

そして、Ｘの送信を行った後は、ウェアラブル・デバイス３００は、再び待機状態すなわち受信待ち状態に遷移し、タッチネット送信部３０１を電源オフにするとともにタッチネット受信部３０２を電源オンにする（ステップ１９１１）。

【０２１７】

周辺デバイス３２０側では、タッチネット伝送によりＸを受信すると（ステップ１９０３）、チャレンジ・キーとＸとから、ウェアラブル・デバイス３００が所有するＩＤ情報を特定して、その正当性を認証する（ステップ１９０４）。そして、受信したＩＤ情報に対応する処理を実行した後（１９０５）。ステップ１９０１に復帰して、次にユーザが接触するまで待機する。但し、ステップ１９０５で行う処理自体に関しては、後述に譲る。

【０２１８】

他方、Ｘの受信に失敗したときには（ステップ１９０３）、周辺デバイス３２０は、接触したユーザに対する処理を行うことなく、ステップ１９０１に復帰して、次にユーザが接触するまで待機する。

【０２１９】

図１９に示すような認証処理手順によれば、ウェアラブル・デバイス３００と周辺デバイス３２０との間でＩＤ情報そのものを伝送することなく、ウェアラブ

ル・デバイス３００が正当なＩＤを所有していることを認証することができる、という点を充分理解されたい。

【０２２０】

本実施例に係る認証情報通信システム及び認証情報通信方法によれば、パスワード入力のような煩雑なユーザ操作を行うことなく、操作する機器にユーザが手を触れるだけで確実且つ安全に利用者認証を行うことができる。

【０２２１】

より具体的に、以下の事柄を実現することができる。

（１）他人のコンピュータや携帯電話等を使っても取引をしても、機器の所有者ではなく、機器を操作している人の口座に課金する。

（２）自動販売機、公衆電話、キオスク端末など、不特定多数が扱う機器でも、操作した人に対して課金する。

（３）権利又は権限のある人が触るとロックが解除される（あるいは権限のないものが触るとロックされ又はロックが解除されない）ドア・ノブやドロワを作成する。

（４）権利又は権限のある人がハンドルに触れていないと、エンジンが始動しない自動車を実現する。

（５）テレビ受像機やＷｅｂブラウザのリモコンに、「その人がよく見る番組（又はよく閲覧するＷｅｂページ）」に切り替わるボタンを取り付けたりして、特定ユーザの嗜好や操作履歴に適応した処理を行う。

（６）マウスに触れると、そのユーザの操作環境に自動的に切り替わるコンピュータ（又はそのユーザ・インターフェース）を実現する。例えば、マウスを持っているユーザが所有する（権限を持つ）ファイルにアクセスする。

（７）テレビ・ゲームのゲーム・パッドやコントローラに触れると、その人向けに設定が切り替わる（例えば、既にクリアしたステージ、ゲームの履歴情報や、難易度設定など）。

（８）ペット・ロボットに触れると、そのロボットの所有者（又は正当なユーザ）か否かを認証し、その認証結果に基づく挙動を実行する。

【０２２２】

以下では、ウェアラブル・デバイス３００経由で認証並びに識別されたユーザごとに対応したサービスを提供する例について詳解する。

【０２２３】

（Ａ）パブリック・スペースでのインターネット・アクセス

例えば、空港のロビーや待合室、駅のホーム、ガソリン・スタンド、コンビニエンス・ストアなどのパブリック・スペースに、誰もが手に触れることができる街頭端末が設置されているとする。

【０２２４】

この街頭端末はネットワーク接続されている。そして、ウェアラブル・デバイスを装着したユーザがこの街頭端末の電極に触れることで、ウェアラブル・デバイスと街頭端末の間で、所定の認証・識別手続が実行される（図１８又は図１９を参照のこと）。

【０２２５】

認証手続に成功すると、街頭端末は、ウェアラブル・デバイスが持つ識別情報によって特定されたユーザ・アカウントを基にログインを許容する。また、街頭端末は、ユーザのログインとともに、そのままインターネットにアクセスする。

【０２２６】

このとき、街頭端末上には、ポータル・サイトにアクセスしてもよいし、あるいはメール・ソフトを起動してもよい。ここで言うポータル・サイトは、街頭端末上で設定された省略時のサイトであってもよいし、あるいはユーザ・アカウントなどから引き出された個人情報や操作履歴に基づいて決定されるサイトであってもよい。または、ユーザ・アカウントに相当するメール・ボックスにアクセスして、受信状況（例えば、"Mr. ****, you have 10 mails"など）を表示するようにしてもよい。

【０２２７】

なお、認証手続に成功したときに、街頭端末又はウェアラブル・デバイスは、特定のビープ音を発生する、あるいは画面上に特定のアニメーションを表示するなどして、シンボリックなユーザ・フィードバックを与えるようにしてもよい。ユーザは、このような事象の発生後、ユーザは認証手続が終了したことやインタ

ーネット接続料などの課金の開始を意識することができる。

【０２２８】

街頭端末自体は不特定多数のユーザが扱う機器であり課金の対象とすることはできないが、本実施例によれば、ウェアラブル・デバイス経由で街頭端末の操作者を逐次特定することができるので、操作者自体を課金の対象とすることができる（例えば、操作者の口座から利用料を引き落とす）。

【０２２９】

ユーザによっては、ログイン中に街頭端末から離れてしまい、ログアウトの手続を忘れることがある。また、このような場合、不正ユーザによる「なりすまし」などの悪用が行われる危険があり、ユーザに対して不測の利用料が課金されるおそれがある。街頭端末はパブリック・スペースで利用されるゆえ、なりすましの危険はとりわけ高い。

【０２３０】

このような事態に備えて、街頭端末は、認証済みのユーザからの最後のアクセスから一定時間が経過することによって自動的にログアウト手続を行うようにしてもよい。あるいは、別のＩＤ情報を持ったユーザすなわちウェアラブル・デバイスでアクセスされたことに応答して、直前まで継続していたセッションを終了して、再度認証・識別処理を開始して、別のセッションとしてログインを行うようにしてもよい。ウェアラブル・デバイスすなわちＩＤ情報を持たないユーザからアクセスがあったときも、同様に直前のセッションを終了するようにしてもよい。

【０２３１】

（Ｂ）ウェアラブル・デバイスを媒介とした権限の委譲

例えば、ホテルのロビーや、レンタカー店の窓口など、部屋や乗用者などに対する使用権など権限の委譲を受けるような場面を想定する。ここでは、ロビーのカウンタなどが電極として作用する。

【０２３２】

ウェアラブル・デバイスを装着したユーザは、ホテルのチェックイン・カウンタでブースに触れることにより、認証・識別、予約確認、チェックイン手続など

の各種手続が自動的に且つ暗黙のうちにウェアラブル・デバイス経由で実行される。

【０２３３】

認証手続に成功すると、カウンタに備え付けのディスプレイ、あるいはウェアラブル・デバイス上に搭載されたディスプレイ上に、委譲された権限の内容を表示するようにして、ユーザに対してシンボリックなフィードバックを与えるようにしてもよい。ここで言う権限内容には、例えば、宿泊することができた客室のルーム・ナンバーと宿泊期間であってもよいし、借りることができた乗用車のナンバーと返却期限であってもよい。

【０２３４】

また、認証手続に成功すると、ウェアラブル・デバイス側には、所定の権限情報がダウンロードされる。この権限情報は、例えば、ホテルの貸室の鍵情報、あるいは乗用者の鍵情報と等価な役割を持っている。すなわち、権限情報を担持したウェアラブル・デバイスを装着していれば、ユーザは部屋あるいは乗用車のドア・ノブに手をかけるだけで、ウェアラブル・デバイス経由で認証手続が暗黙のうちに行われ、ドアをそのまま開くことができる。

【０２３５】

（Ｃ）情報資源へのアクセス

例えば、ホテルの客室内にはパーソナル・コンピュータ（ＰＣ）が設置されており、マウスやキーボード、ディスプレイ筐体の表面などが電極を兼ねているとする。

【０２３６】

ウェアラブル・デバイスを装着したユーザは、例えばマウスに触れるだけで、自動的で且つ暗黙のうちに認証手続並びに識別手続が実行される。

【０２３７】

そして、認証処理並びに識別処理が成功裏に終わると、ＰＣ画面上では、識別情報に基づいてそのユーザの操作環境（ユーザ・プレファレンス）に自動的に切り替わる。

【０２３８】

また、マウスを持っているユーザが所有する（すなわち権限を持つ）ファイルにアクセスすることができる。

【０２３９】

例えば、ＰＣがインターネットのような広域ネットワークに接続されている場合には、リモート・ディスクからファイルやその他の情報資源を安全に取り出すことができる。したがって、ユーザは、必要なファイルをフロッピー・ディスクやメモリ・カードなどの記録媒体に逐次コピーして持ち歩かなくても、いつもと同じ操作環境上でファイル・アクセスすることができる。

【０２４０】

あるいは、会議室などにおいて、スライド投影用のスクリーン（壁面）や、投影画像を指示するためのポインタが電極を兼ねていてもよい。

【０２４１】

この場合、ウェアラブル・デバイスを装着したユーザは、例えばスクリーンやポインタに触れるだけで、自動的で且つ暗黙のうちに認証手続並びに識別手続が実行される。

【０２４２】

そして、認証処理並びに識別処理が成功裏に終わると、会議室に設置された情報端末上から、ユーザが所有するファイル（例えばプレゼンテーション資料用のファイル）にアクセスすることができる。

【０２４３】

例えば、会議室内の情報端末がインターネットのような広域ネットワークに接続されている場合には、リモート・ディスクからファイルやその他の情報資源を安全に取り出すことができる。したがって、ユーザは、必要なファイルをフロッピー・ディスクやメモリ・カードなどの記録媒体に逐次コピーして持ち歩かなくても、いつもと同じ操作環境上でファイル・アクセスすることができる。

【０２４４】

（Ｄ）情報コンテンツの購入・再生

画像や音響などほとんどのメディアがデジタル化され、コンピュータ上で再生可能なデータ・コンテンツとして、市場で流通・取引されている。例えば、自動

販売機上で、データ・コンテンツを取り扱ってもよい。

【０２４５】

例えば、ＫＩＯＳＫ端末などの自動販売機上のメニュー画面が電極を兼ねているとする。ウェアラブル・デバイスを装着したユーザは、メニュー画面上で、所望のコンテンツを指示するだけで、自動的に且つ暗黙のうちに認証手続並びに識別手続が実行される。

【０２４６】

そして、認証処理並びに識別処理が成功裏に終わると、ユーザが装着したウェアラブル・デバイス上には、どのコンテンツを購入したかという購入情報が書き込まれる。

【０２４７】

但し、購入したコンテンツ自体をウェアラブ・デバイス上にダウンロードする必要は必ずしもない。例えば、コンテンツ販売機に接続されたセンター局において、誰がどのコンテンツを購入したかという購入情報を集中管理するようにしておき、適宜、コンテンツの実体の引渡しを行うようにしてもよい。

【０２４８】

例えば、ユーザはある映画コンテンツを購入したとする。そして、ユーザは、コンテンツ購入後に、壁にモニタが設置されるとともにリモコンが用意されているような、どこかのラウンジ（あるいはホテルの客室）に行くとする。

【０２４９】

リモコンは電極を兼ねており、ユーザがリモコンを拾い上げることにより、ウェアラブル・デバイス経由で認証手続並びに識別手続が自動的で且つ暗黙のうちに実行される。

【０２５０】

そして、認証処理並びに識別処理が成功裏に終わると、識別情報を基にセンター局に問い合わせることで、このユーザが映画コンテンツを購入していたことが識別される。

【０２５１】

このような場合、購入しておいた映画コンテンツが、センター局からラウンジ

に送信され（あるいは、センター局は所定のサーバに対して映画コンテンツの供給を指示し）、ラウンジ内で映画を上映することができる。

【０２５２】

ユーザは、映画コンテンツの購入に際し、ビデオ・テープ・カートリッジやＤＶＤなどのメディアを持ち運ぶ手間を省くことができる。

【０２５３】

［追補］

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２５４】

［注釈］

＊：例えば、「暗号・ゼロ知識証明・数論」（情報処理学会監修／岡本龍明、大田和夫編、共立出版）を参照のこと。

【０２５５】

【発明の効果】

以上詳記したように、本発明の認証情報通信システム及び認証情報通信方法によれば、ユーザが装着した携帯機器と、サービスを提供するサービス提供端末間での認証処理を人体を介する通信によって実行し、それぞれの接点に人体が触れることでデータ通信を可能とした。したがって、ユーザが接触したという物理的実感を確認して認証処理が行なわれ、非接触型の認証システムにおける処理の開始確認の曖昧さが解消され、ユーザの不安感が取り除かれるとともに、カード等の旧来の接触型の認証システムのようなカードの取り出し、センサでの読み取り処理等の煩わしさもなく、ユーザの負担が軽減される優れた認証処理システムが実現される。

【０２５６】

また、本発明の認証情報通信システム及び認証情報通信方法によれば、ユーザ

が装着した携帯機器にユーザ固有のユーザ固有識別子と、サービス端末の提供するサービスに応じて各ユーザごとに生成されるユーザ可変識別子とを格納し、サービス端末から送信されるサービス識別子に応じて、携帯端末において、ユーザ固有識別子とユーザ可変識別子とから認証用のサービス固有ユーザ識別データを生成してサービス端末に送付する構成としたので、サービス識別子で規定した内容に応じたユーザ単位の課金処理等、様々なユーザ管理やサービス管理が実行できる認証処理システムが実現される。

【０２５７】

さらに、本発明の認証情報通信システム及び認証情報通信方法によれば、サービス端末がサービスに応じた可変ユーザＩＤをユーザに対して設定する構成としたので、可変ユーザＩＤのデータにユーザ個々の情報、提供サービスの情報、制限等、各種情報を含ませることが可能になり、携帯機器から受信した可変ユーザＩＤに基づいてサービスの実行やその態様を変更することが可能となる。

【０２５８】

また、本発明の認証情報通信システム及び認証情報通信方法によれば、パスワード入力のような煩雑なユーザ操作を行うことなく、操作する機器にユーザが手を触れるだけで確実且つ安全に利用者認証を行うことができる。より具体的に、以下の事柄を実現することができる。

（１）他人のコンピュータや携帯電話等を使っても取引をしても、機器の所有者ではなく、機器を操作している人の口座に課金する。

（２）自動販売機、公衆電話、キオスク端末など、不特定多数が扱う機器でも、操作した人に対して課金する。

（３）権利又は権限のある人が触るとロックが解除される（あるいは権限のないものが触るとロックされ又はロックが解除されない）ドア・ノブやドロワを作成する。

（４）権利又は権限のある人がハンドルに触れていないと、エンジンが始動しない自動車を実現する。

（５）テレビ受像機やＷｅｂブラウザのリモコンに、「その人がよく見る番組（又はよく閲覧するＷｅｂページ）」に切り替わるボタンを取り付けたりして、特

定ユーザの嗜好や操作履歴に適応した処理を行う。

（６）マウスに触れると、そのユーザの操作環境に自動的に切り替わるコンピュータ（又はそのユーザ・インターフェース）を実現する。例えば、マウスを持っているユーザが所有するファイルにアクセスする。

（７）テレビ・ゲームのゲーム・パッドやコントローラに触れると、その人向けに設定が切り替わる（例えば、既にクリアしたステージ、ゲームの履歴情報や、難易度設定など）。

（８）ペット・ロボットに触れると、そのロボットの所有者（又は正当なユーザ）か否かを認証し、その認証結果に基づく挙動を実行する。

【０２５９】

本発明に係る認証情報通信システムによれば、従来はパスワードや鍵などで管理されていた個人情報を、単一の装着型デバイスを用いて集中管理することができる。

【図面の簡単な説明】

【図１】

本発明の認証情報通信システムの基本構成を示すブロック図である。

【図２】

１ＭＨｚ～３０ＭＨｚの範囲でスペクトラムアナライザを用いて測定した人体の伝送特性（両手間）を示す特性図である。

【図３】

電解強度とアンテナからの距離との関係を説明する特性図である。

【図４】

本発明の認証情報通信システムの認証処理におけるユーザ側の携帯機器における処理を説明する図である。

【図５】

本発明の認証情報通信システムの認証処理におけるサービス端末における処理を説明する図である。

【図６】

本発明の認証情報通信システムにおける携帯機器の機器構成例を示す図である

。

【図７】

本発明の認証情報通信システムにおける携帯機器における処理フローを説明する図である。

【図８】

本発明の認証情報通信システムにおけるサービス端末における処理フロー（その１）を説明する図である。

【図９】

本発明の認証情報通信システムにおけるサービス端末における処理フロー（その２）を説明する図である。

【図１０】

本発明の認証情報通信システムの使用例（その１）を説明する図である。

【図１１】

本発明の認証情報通信システムの使用例（その２）を説明する図である。

【図１２】

本発明の認証情報通信システムにおける第２実施例の構成を示すブロック図である。

【図１３】

本発明の認証情報通信システムにおける第２実施例のサービス登録端末での処理例を示す図である。

【図１４】

本発明の認証情報通信システムにおける第２実施例の課金認証データ記憶部の登録テーブルの例を示す図である。

【図１５】

本発明の認証情報通信システムにおける第２実施例のサービス提供端末での処理例を示す図である。

【図１６】

本発明の認証情報通信システムにおけるその他の実施例の使用例を示す図である。

【図１７】

本発明の第３の実施例に係る認証情報通信システムの機能構成を模式的に示した図である。

【図１８】

ウェアラブル・デバイス３００と周辺デバイス３２０間で行われる認証手続を示したフローチャートである。

【図１９】

ウェアラブル・デバイス３００と周辺デバイス３２０間で行われるゼロ知識証明を利用した認証手続を示したフローチャートである。

【符号の説明】

１０　携帯機器
１１　ＣＰＵ
１２　ＲＡＭ
１３　ＲＯＭ
１４　合成部
１５　通信部
１６　固定データ記憶部
１７　可変データ記憶部
１８　接点
２０　サービス端末
２１　ＣＰＵ
２２　ＲＡＭ
２３　ＲＯＭ
２４　認証部
２５　通信部
２６　認証用ユーザ識別子生成部
２７　認証データ記憶部
２８　サービス識別子保持部
４１　携帯機器

４２　接点

４４　サービス端末

４６　交換機

１１０　サービス提供端末

１１６　接点

１１７　サービス識別子記憶部

１２０　サービス登録端末

１２６　ユーザ識別子生成部

１２７　サービス選択部

１２８　接点

１３０　クリアリングハウス

１３５　認証部

１３６　課金認証データ記憶部

２０１，２０２　携帯装置

３００　ウェアラブル・デバイス

３０１　タッチネット送信部

３０２　タッチネット受信部

３０３　ＣＰＵ

３０４　メモリ

３２０　周辺デバイス

３２１　タッチネット送信部

３２２　タッチにネット受信部

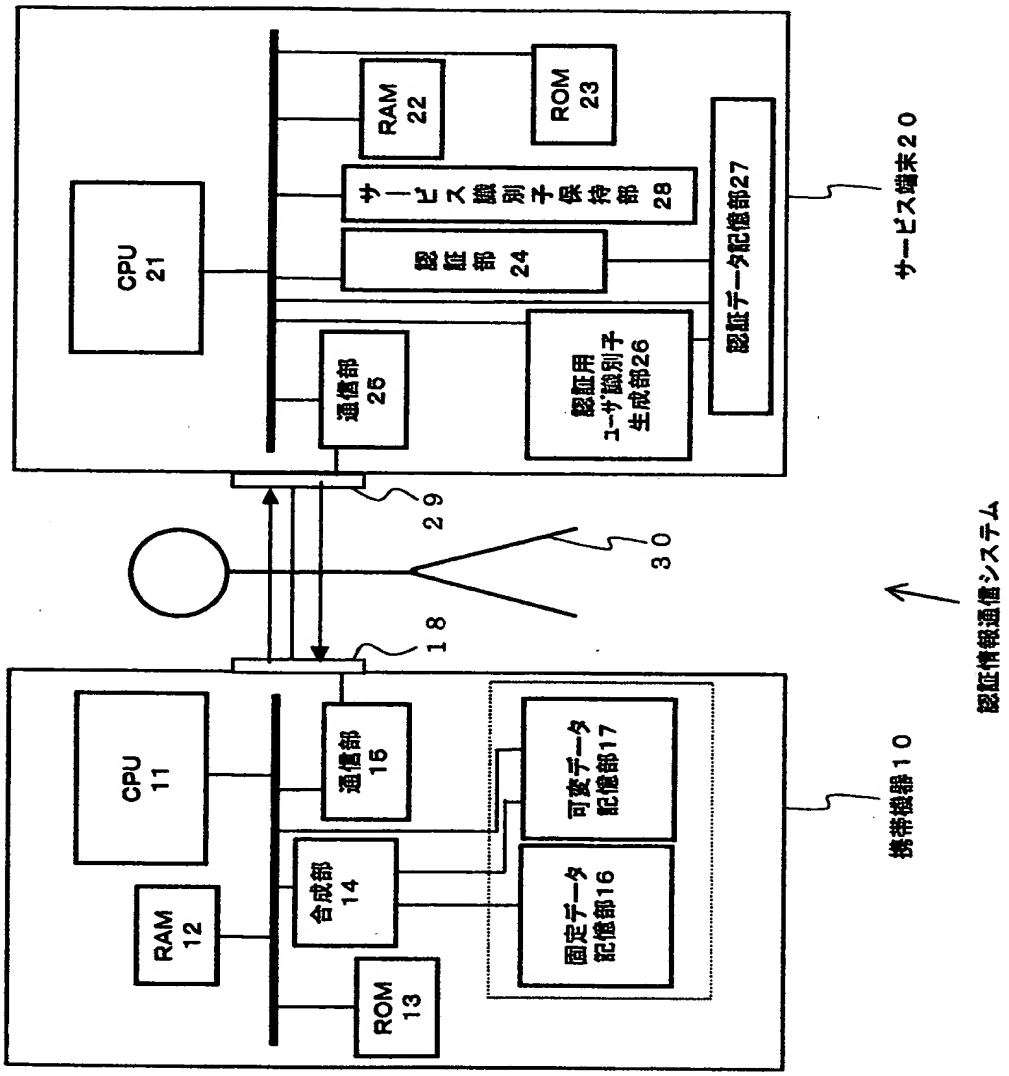
３２３　ＣＰＵ

３２４　メモリ

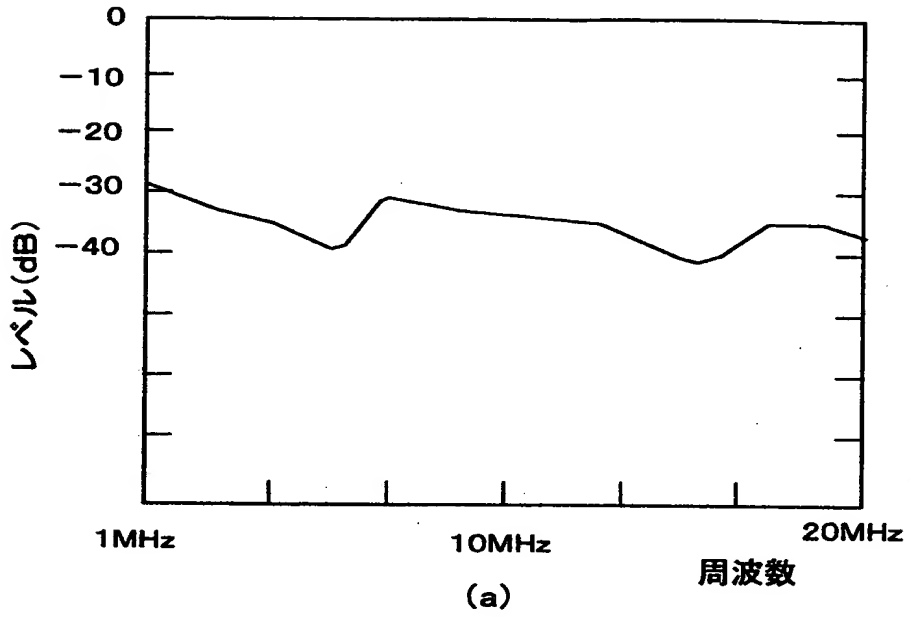
３２５　駆動部

【書類名】　　図面

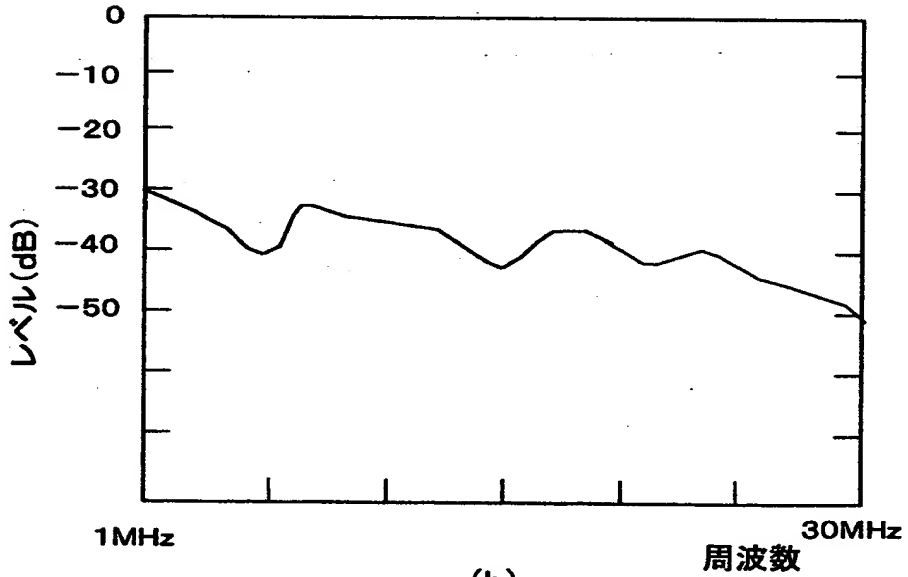
【図１】


CPU
21
RAM
22
ROM
23
サービス識別子保持部
28
認証部
24
通信部
25
認証用
ユーザ識別子
生成部26
認証データ記憶部27
サービス端末２０
２９
３０
１８
認証情報通信システム
CPU
11
RAM
12
ROM
13
通信部
15
合成部
14
可変データ
記憶部17
固定データ
記憶部16
携帯機器１０

【図２】

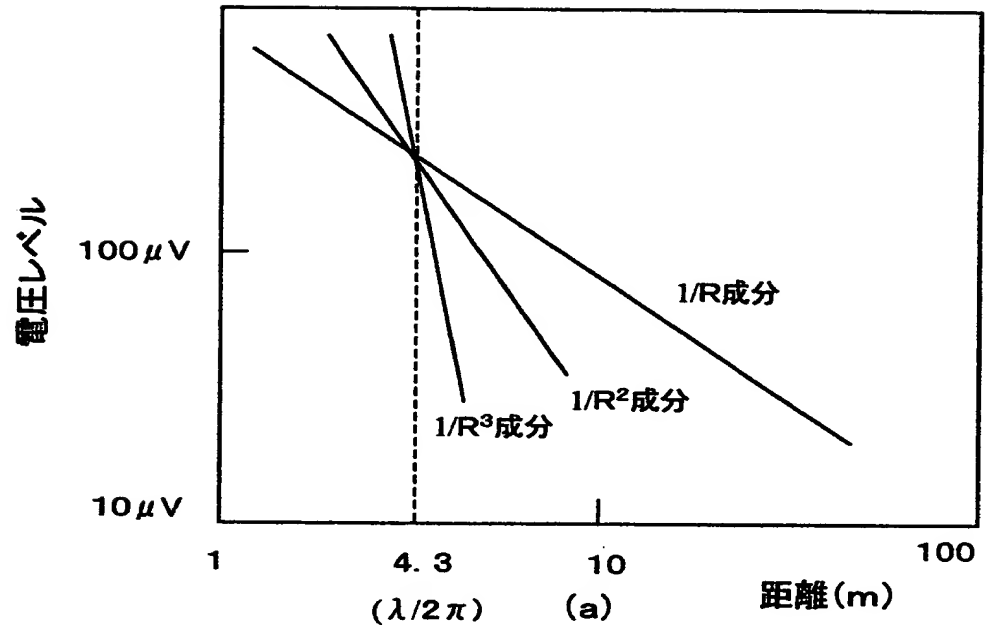

0
−10
−20
−30
−40
レベル(dB)
1MHz
10MHz
20MHz
周波数

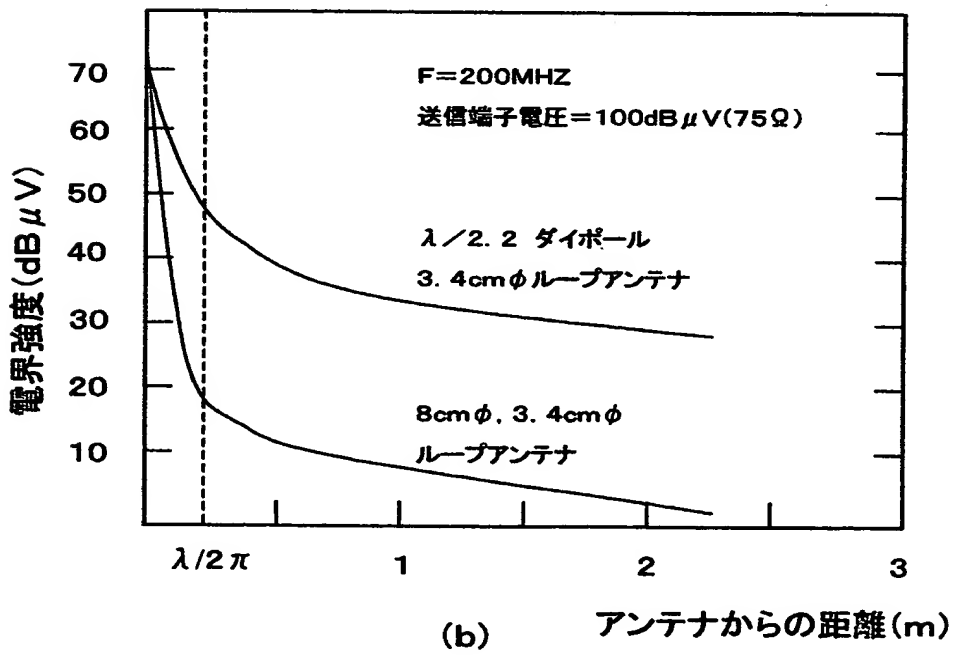
(a)


0
−10
−20
−30
−40
−50
レベル(dB)
1MHz
30MHz
周波数

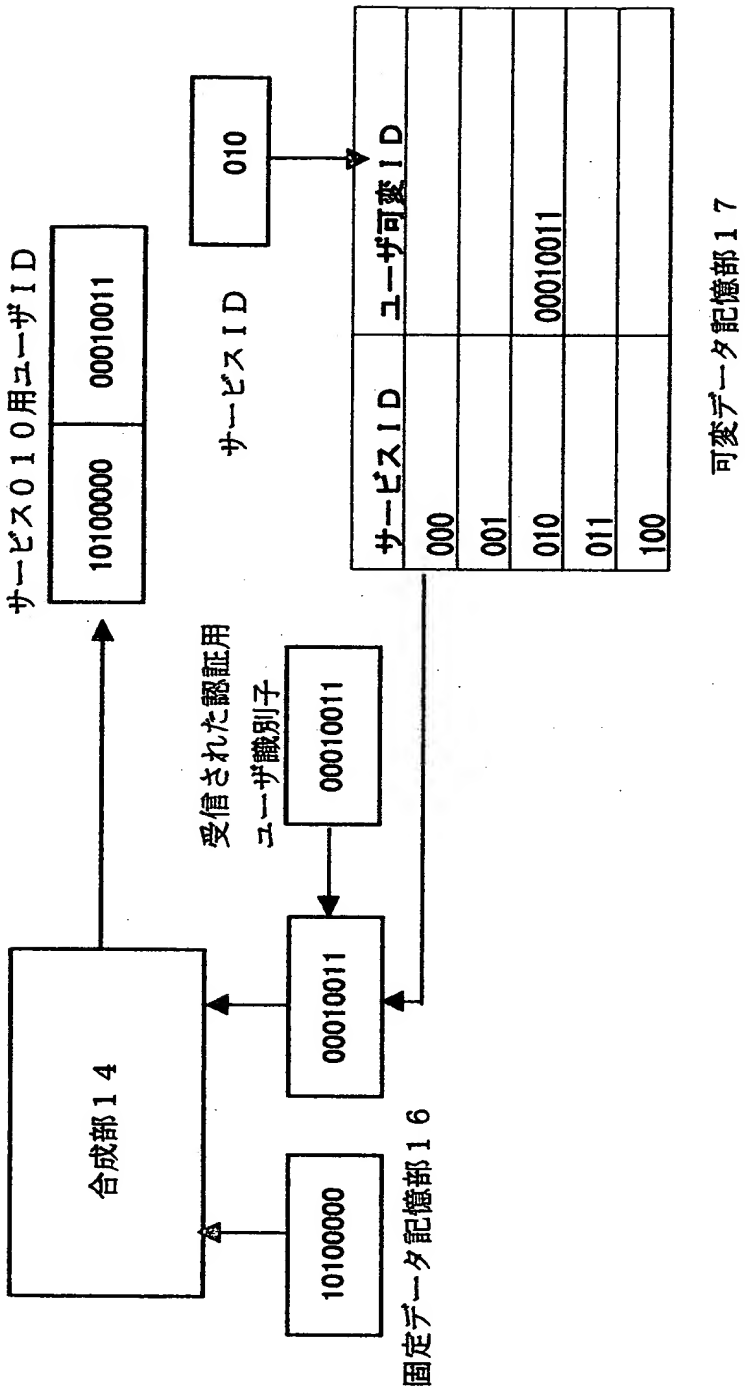
(b)

【図３】

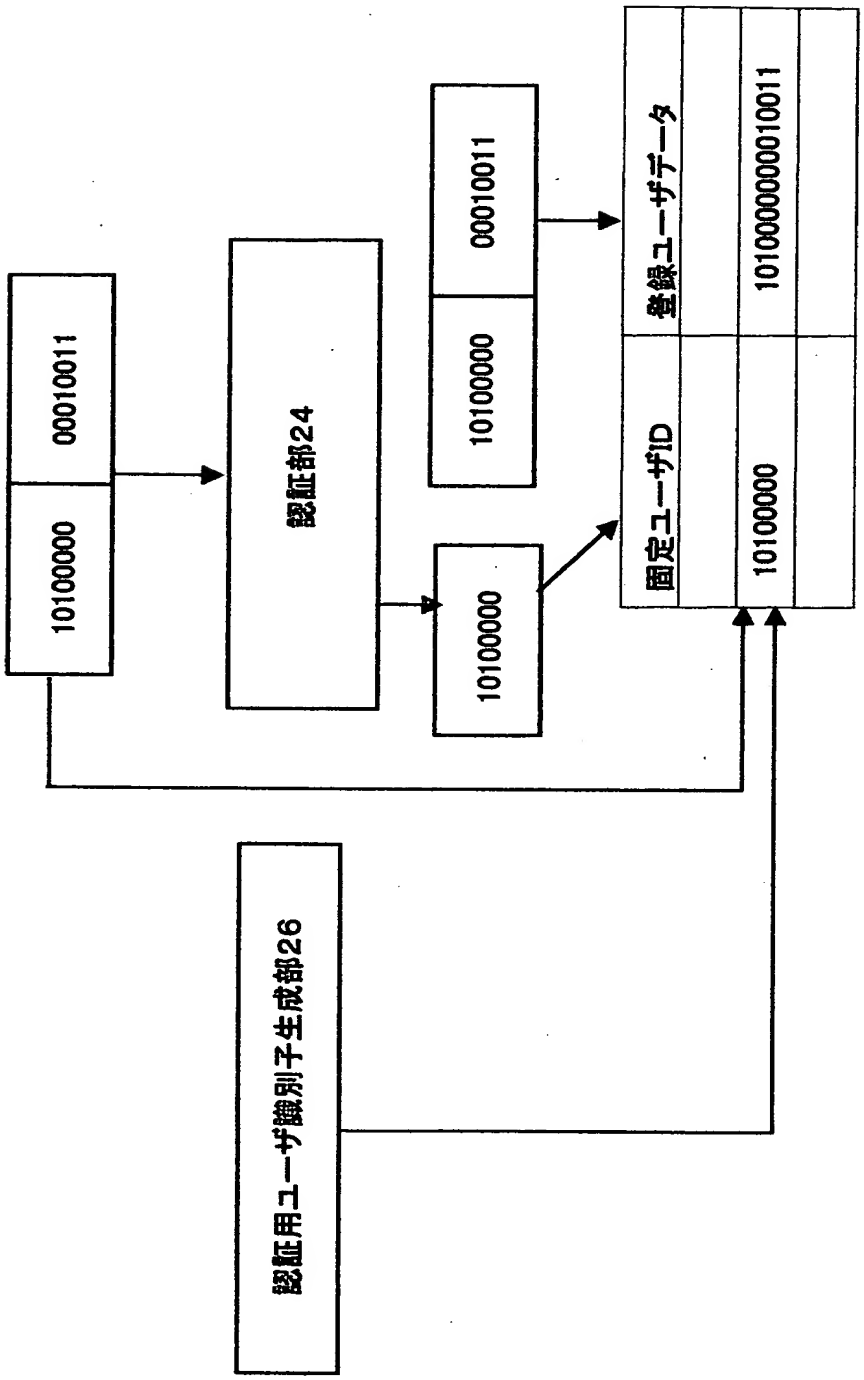

電圧レベル
100μV
10μV
1/R成分
1/R²成分
1/R³成分
1
4.3
(λ/2π)
10
100
(a)
距離(m)


電界強度(dBμV)
70
60
50
40
30
20
10
F=200MHZ
送信端子電圧=100dBμV(75Ω)
λ/2.2 ダイポール
3.4cmφループアンテナ
8cmφ, 3.4cmφ
ループアンテナ
λ/2π
1
2
3
(b)
アンテナからの距離(m)

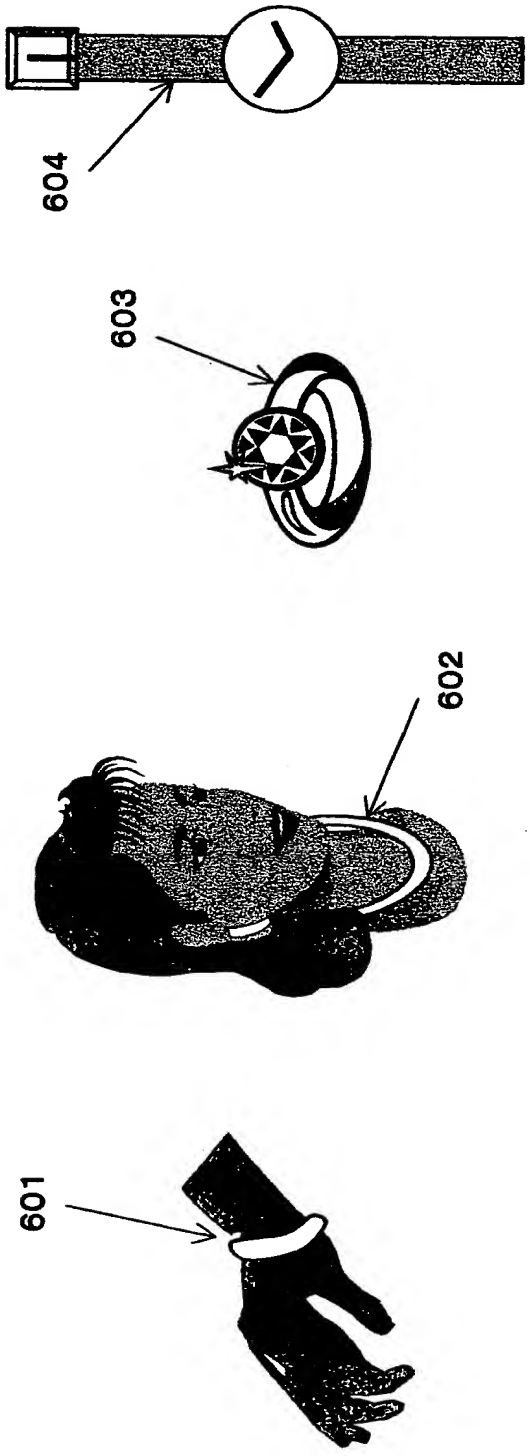
【図４】


サービス０１０用ユーザＩＤ
10100000
00010011
サービスＩＤ
010
サービスＩＤ
ユーザ可変ＩＤ
000
001
010
011
100
00010011
可変データ記憶部１７
受信された認証用
ユーザ識別子
00010011
合成部１４
00010011
10100000
固定データ記憶部１６

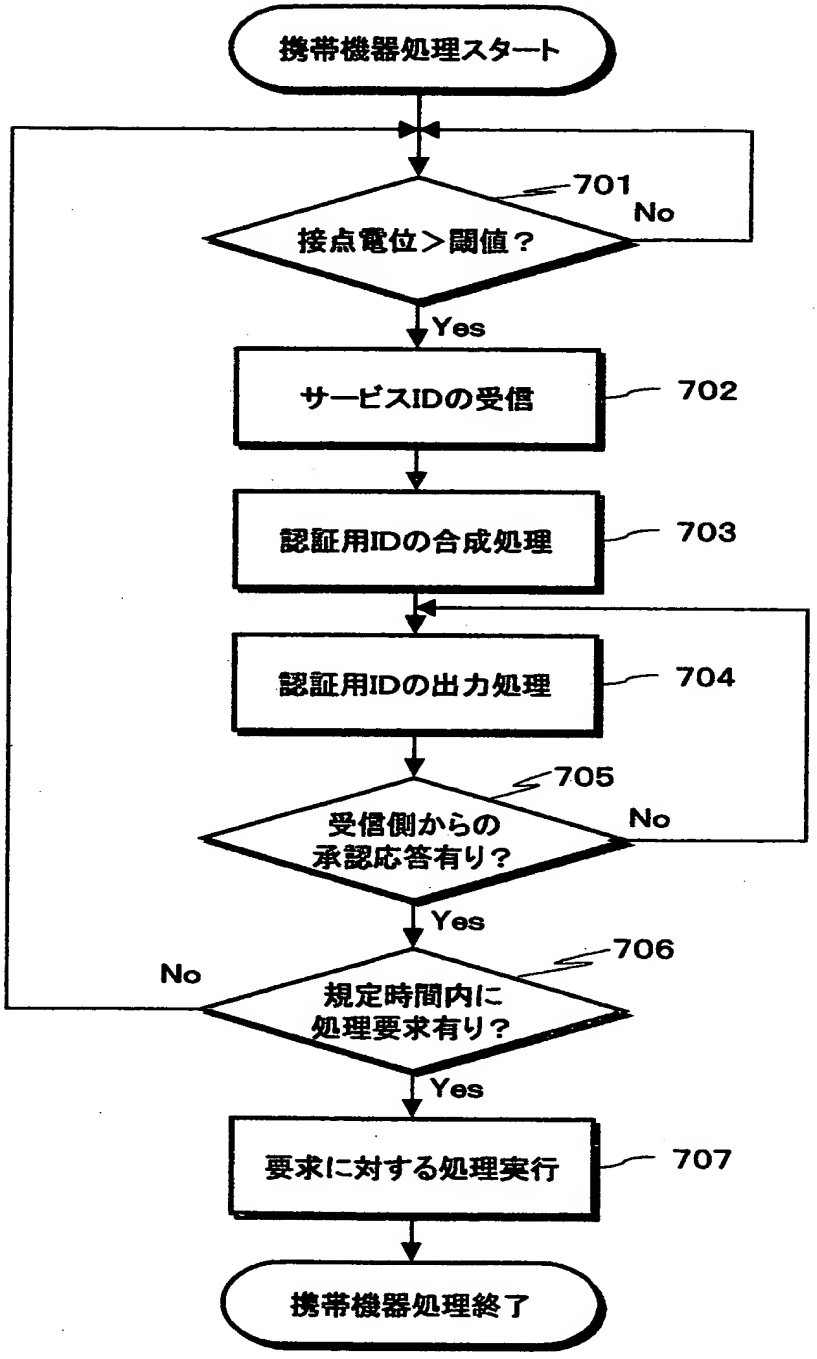
【図５】


10100000
00010011
認証部24
10100000
00010011
10100000
固定ユーザID
登録ユーザデータ
10100000
1010000000010011
認証用ユーザ識別子生成部26

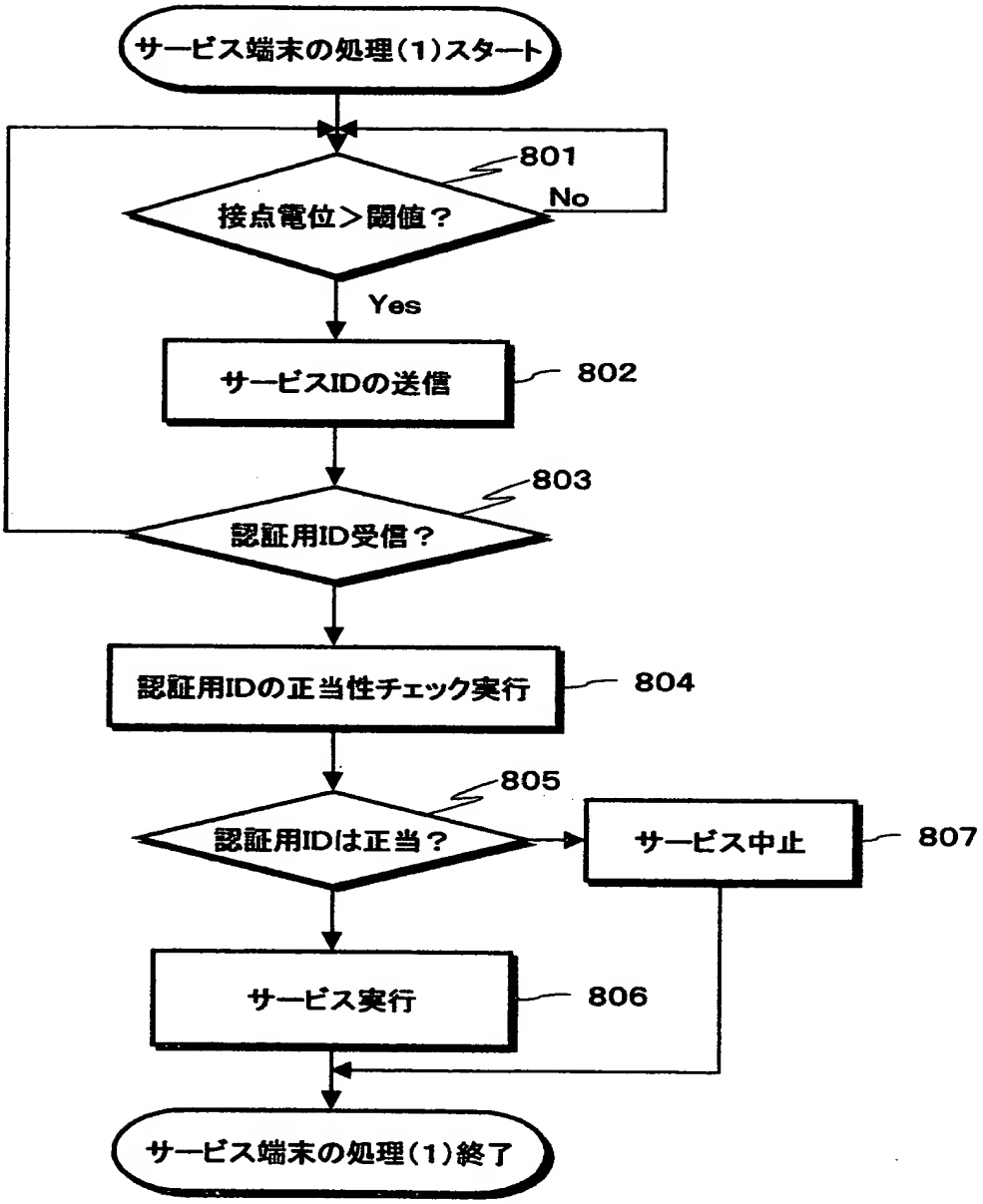
【図６】



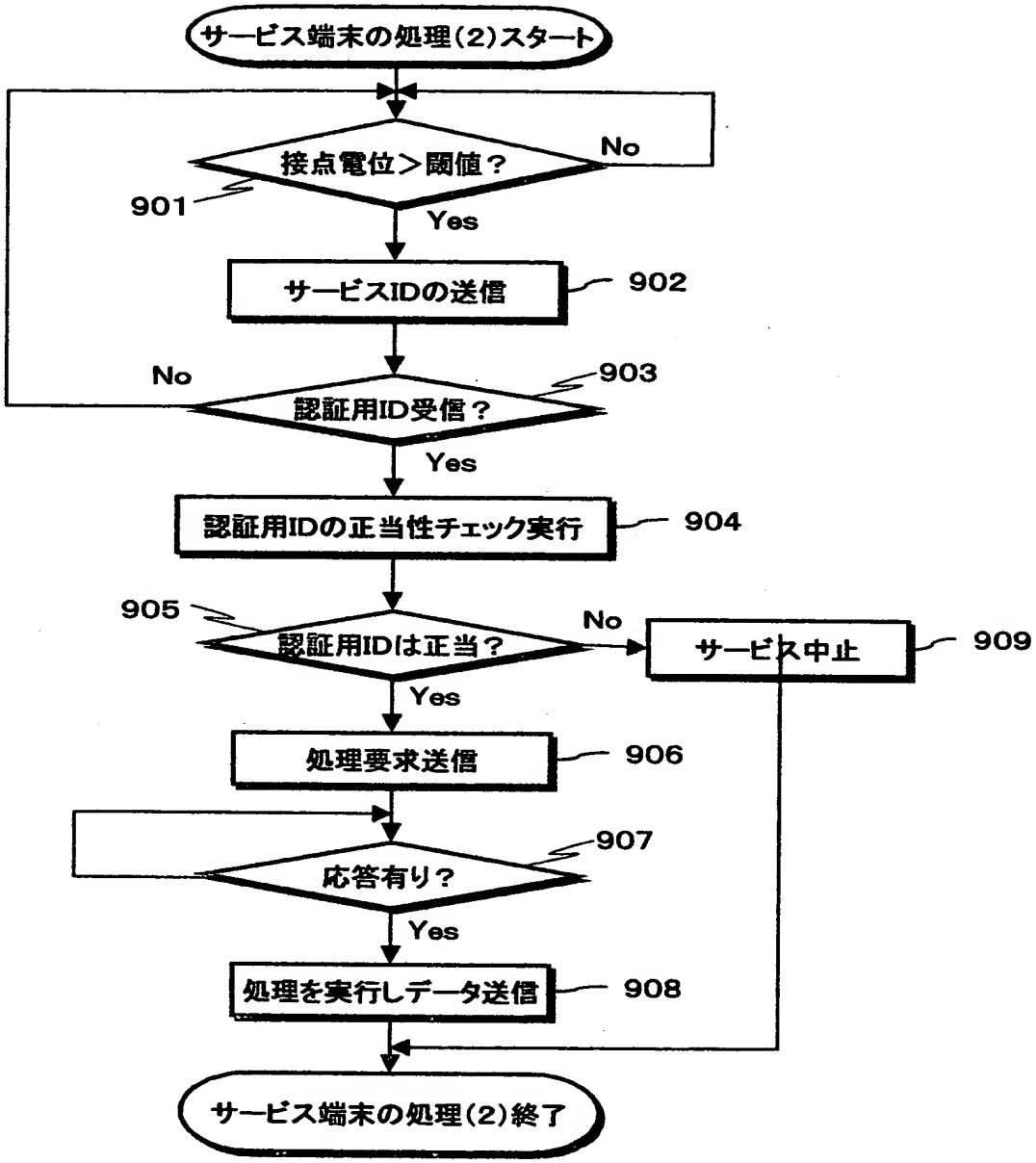
【図７】


携帯機器処理スタート
701
No
接点電位＞閾値？
Yes
サービスIDの受信
702
認証用IDの合成処理
703
認証用IDの出力処理
704
705
No
受信側からの
承認応答有り？
Yes
706
No
規定時間内に
処理要求有り？
Yes
要求に対する処理実行
707
携帯機器処理終了

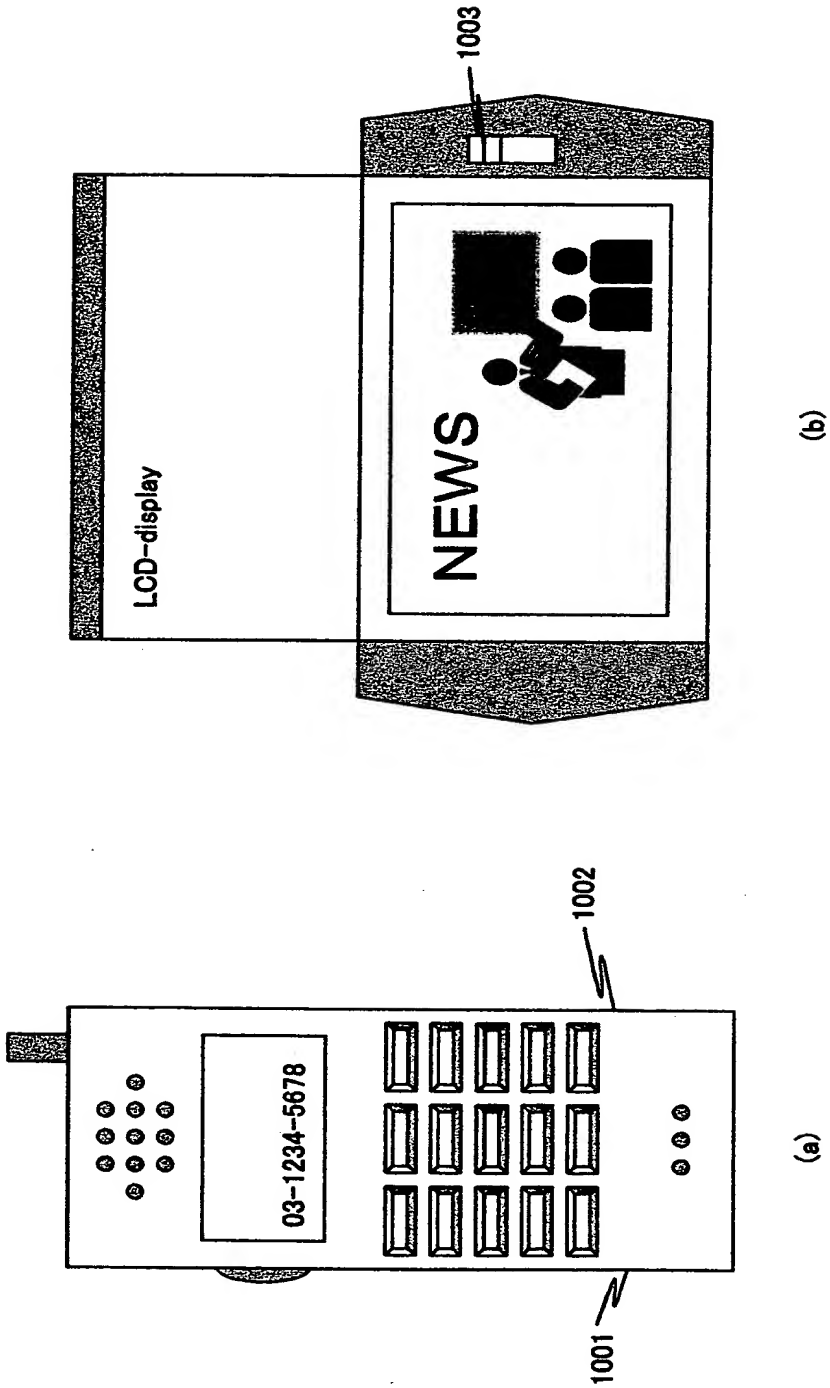
【図８】


サービス端末の処理(1)スタート
801
接点電位＞閾値？
No
Yes
サービスIDの送信
802
803
認証用ID受信？
認証用IDの正当性チェック実行
804
805
認証用IDは正当？
サービス中止
807
サービス実行
806
サービス端末の処理(1)終了

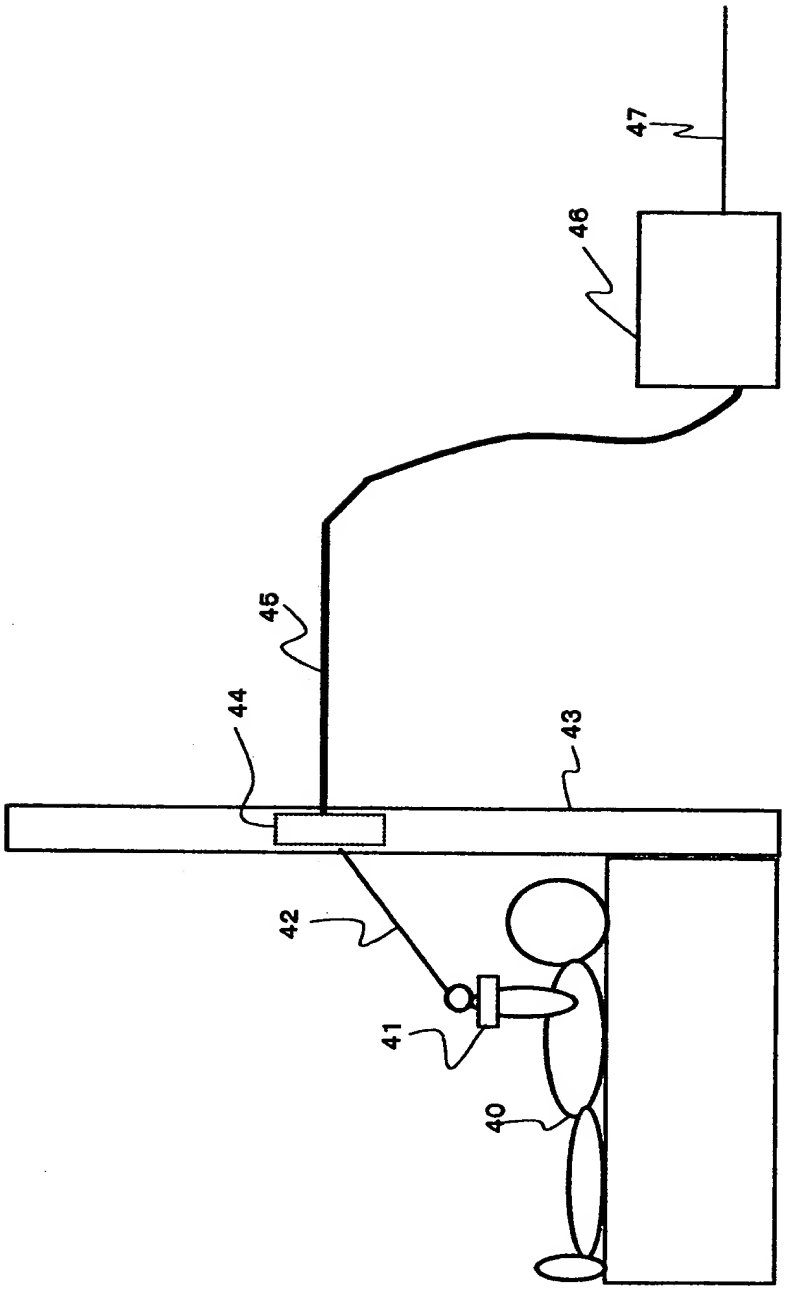
【図９】


サービス端末の処理(2)スタート
接点電位＞閾値？
No
901
Yes
サービスIDの送信
902
No
903
認証用ID受信？
Yes
認証用IDの正当性チェック実行
904
905
認証用IDは正当？
No
サービス中止
909
Yes
処理要求送信
906
907
応答有り？
Yes
処理を実行しデータ送信
908
サービス端末の処理(2)終了

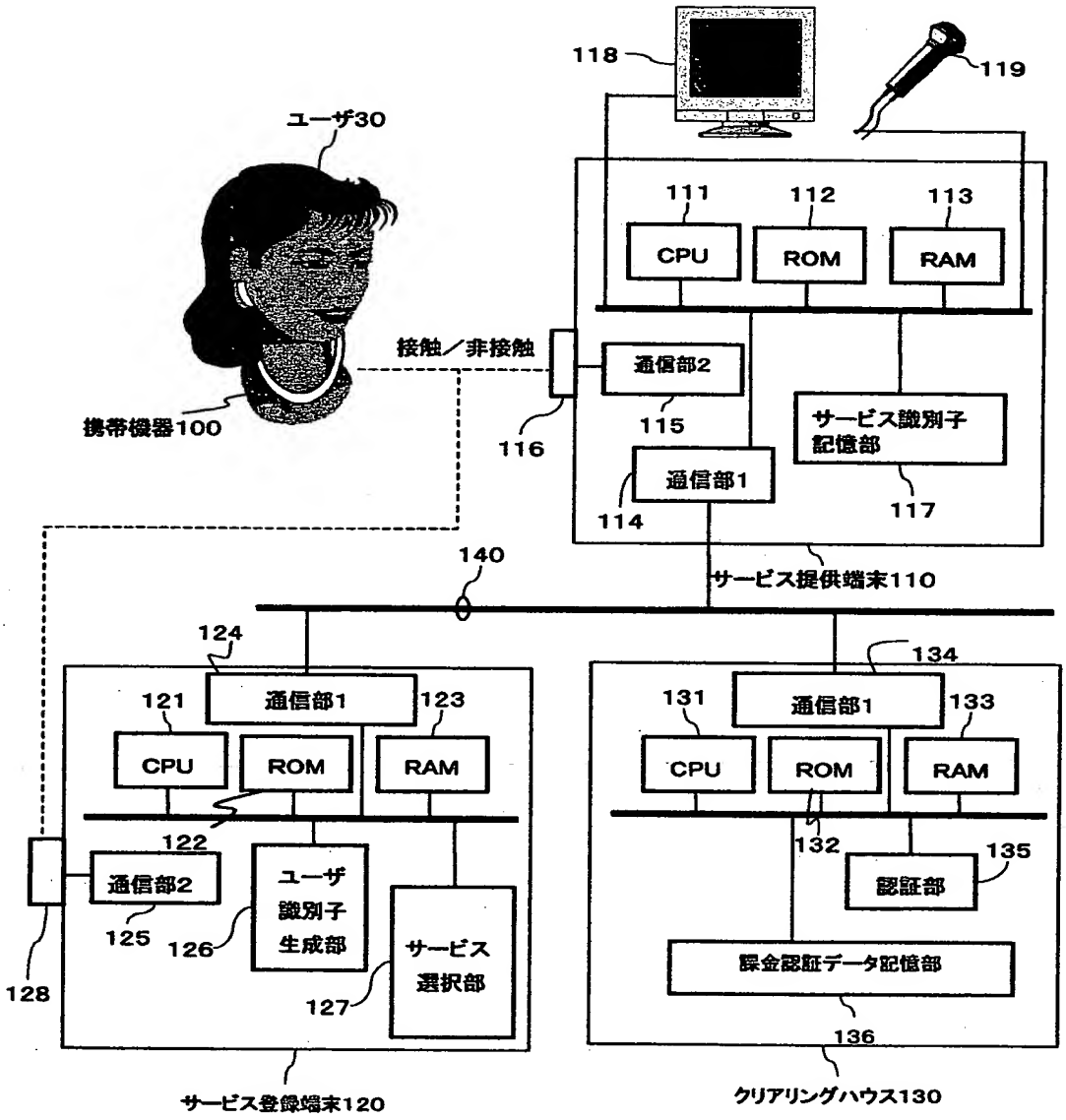
【図１０】



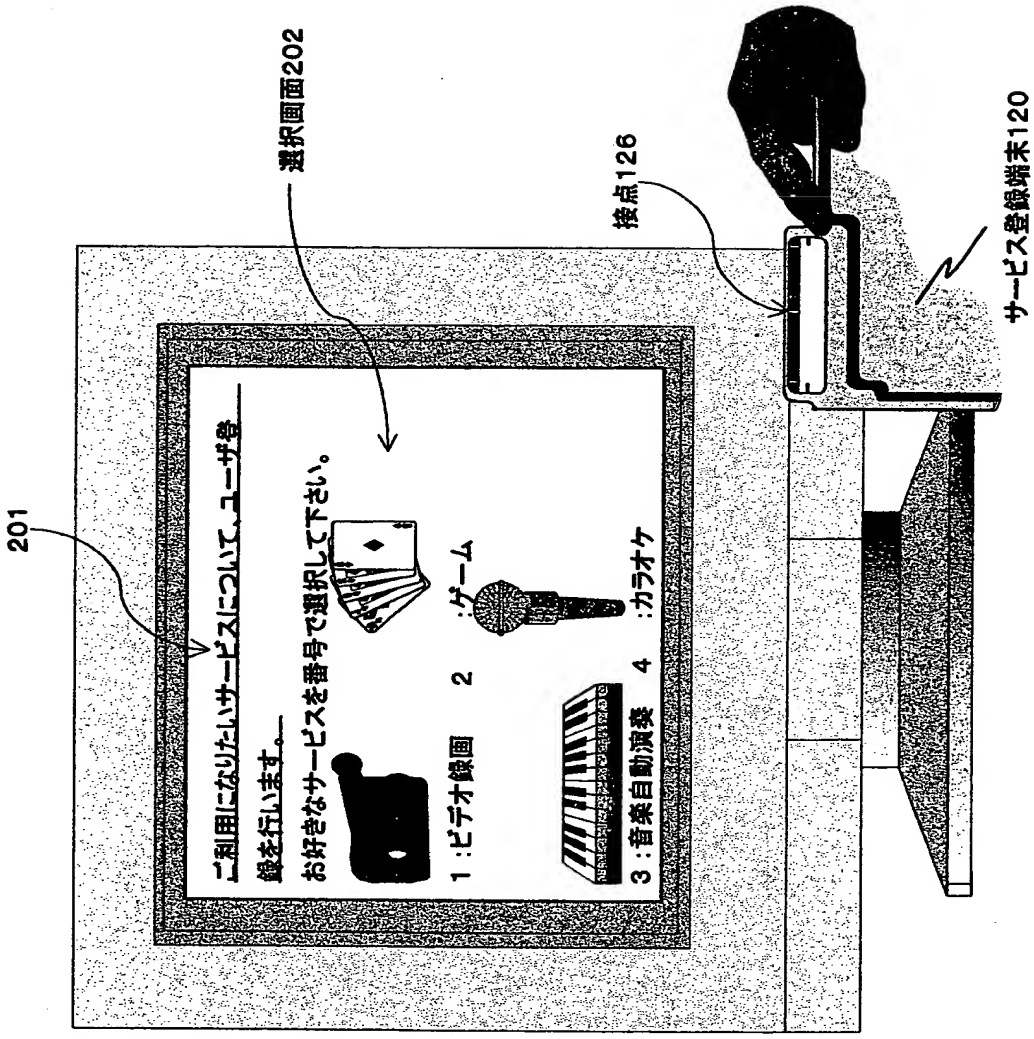
【図１１】



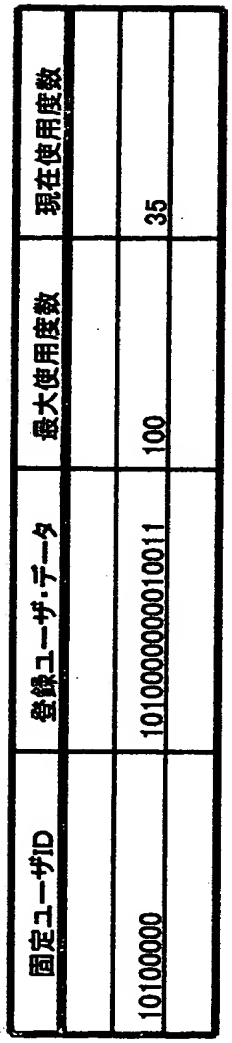
【図１２】


118
119
ユーザ30
111
112
113
CPU
ROM
RAM
接触／非接触
通信部2
115
116
携帯機器100
サービス識別子
記憶部
117
通信部1
114
140
サービス提供端末110
124
134
121
通信部1
123
131
通信部1
133
CPU
ROM
RAM
CPU
ROM
RAM
122
132
135
通信部2
ユーザ
識別子
生成部
認証部
125
126
サービス
選択部
128
127
課金認証データ記憶部
136
サービス登録端末120
クリアリングハウス130

【図１３】

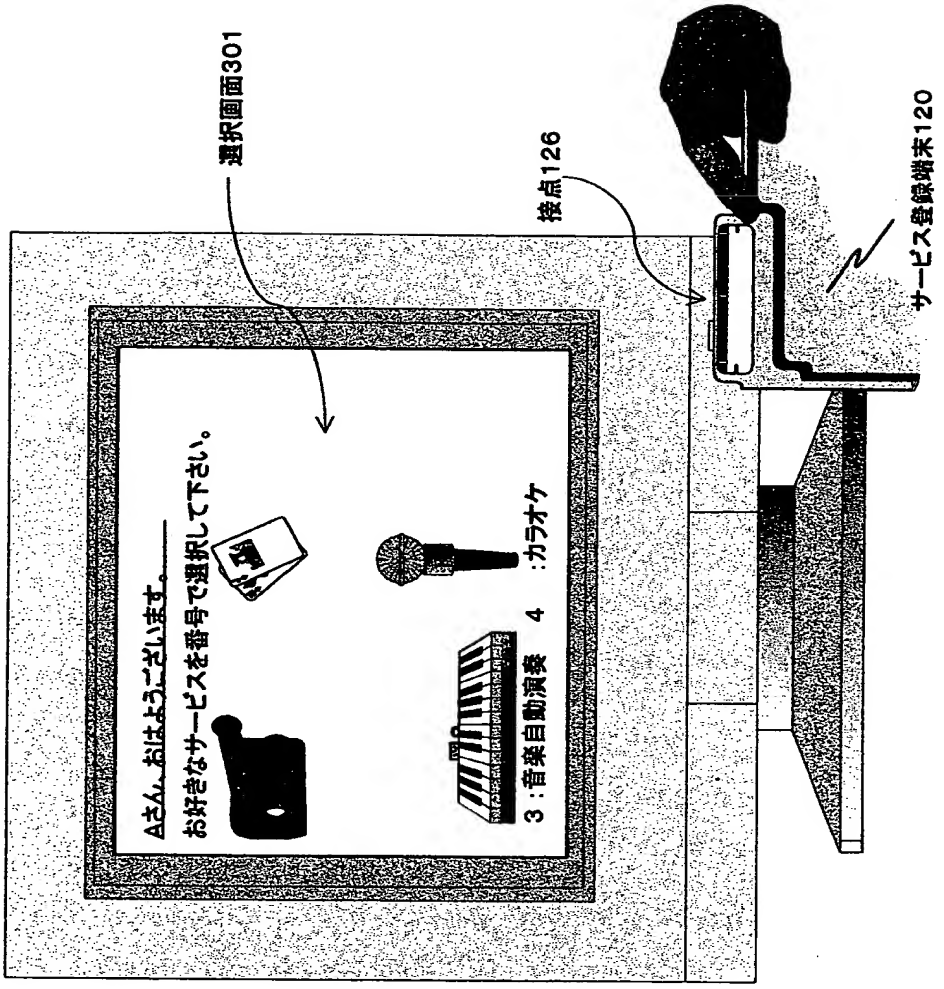

選択画面202
接点126
サービス登録端末120
201
ご利用になりたいサービスについて、ユーザ登
録を行います。
お好きなサービスを番号で選択して下さい。
1：ビデオ録画
2 :ゲーム
3：音楽自動演奏
4 :カラオケ

【図１４】

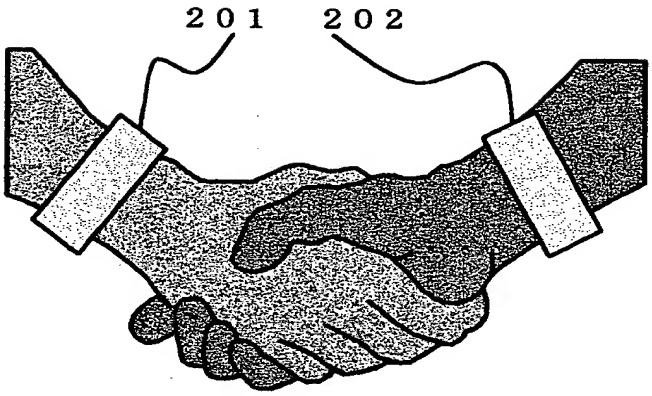


固定ユーザID	登録ユーザ・データ	最大使用度数	現在使用度数
10100000	1010000000010011	100	35

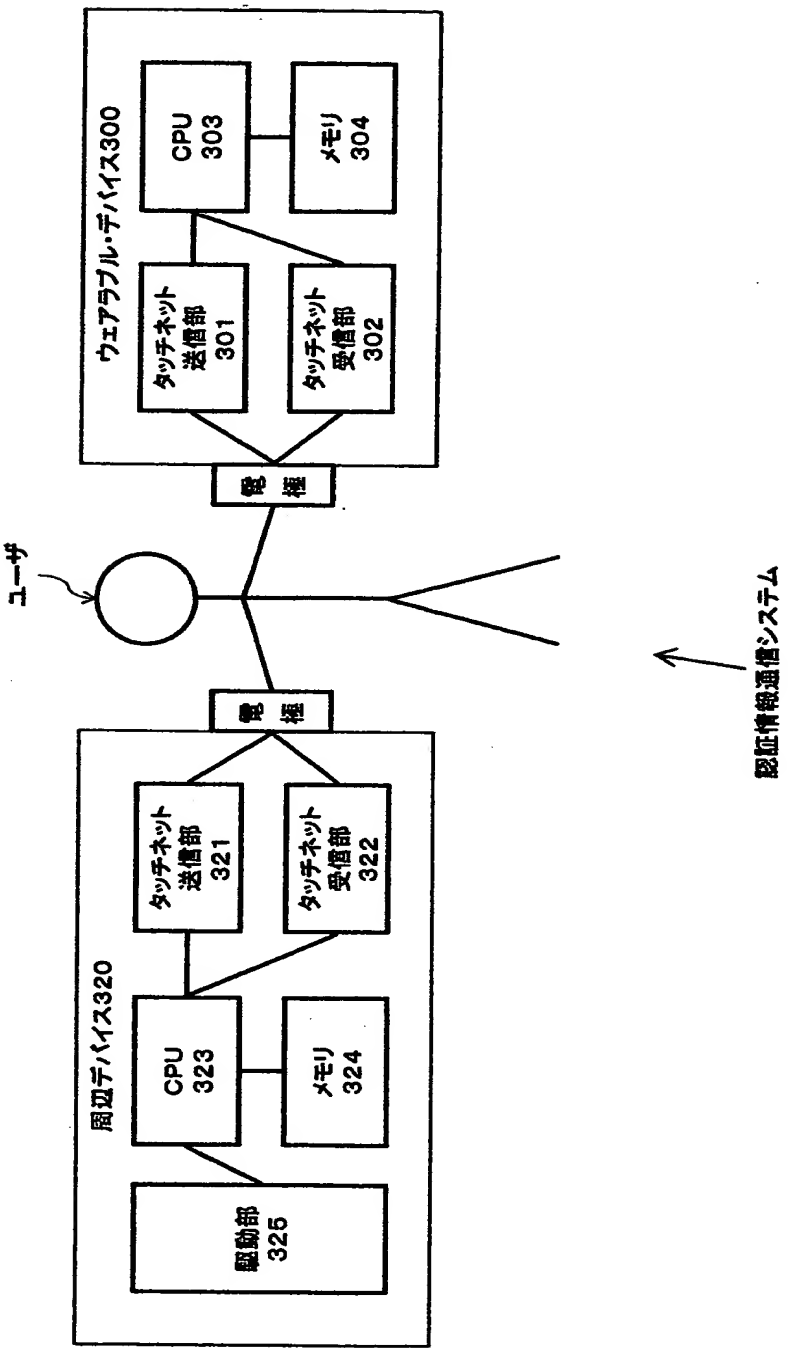
【図１５】


選択画面301
接点126
サービス登録端末120
Aさん、おはようございます。
お好きなサービスを番号で選択して下さい。
3：音楽自動演奏
4　：カラオケ

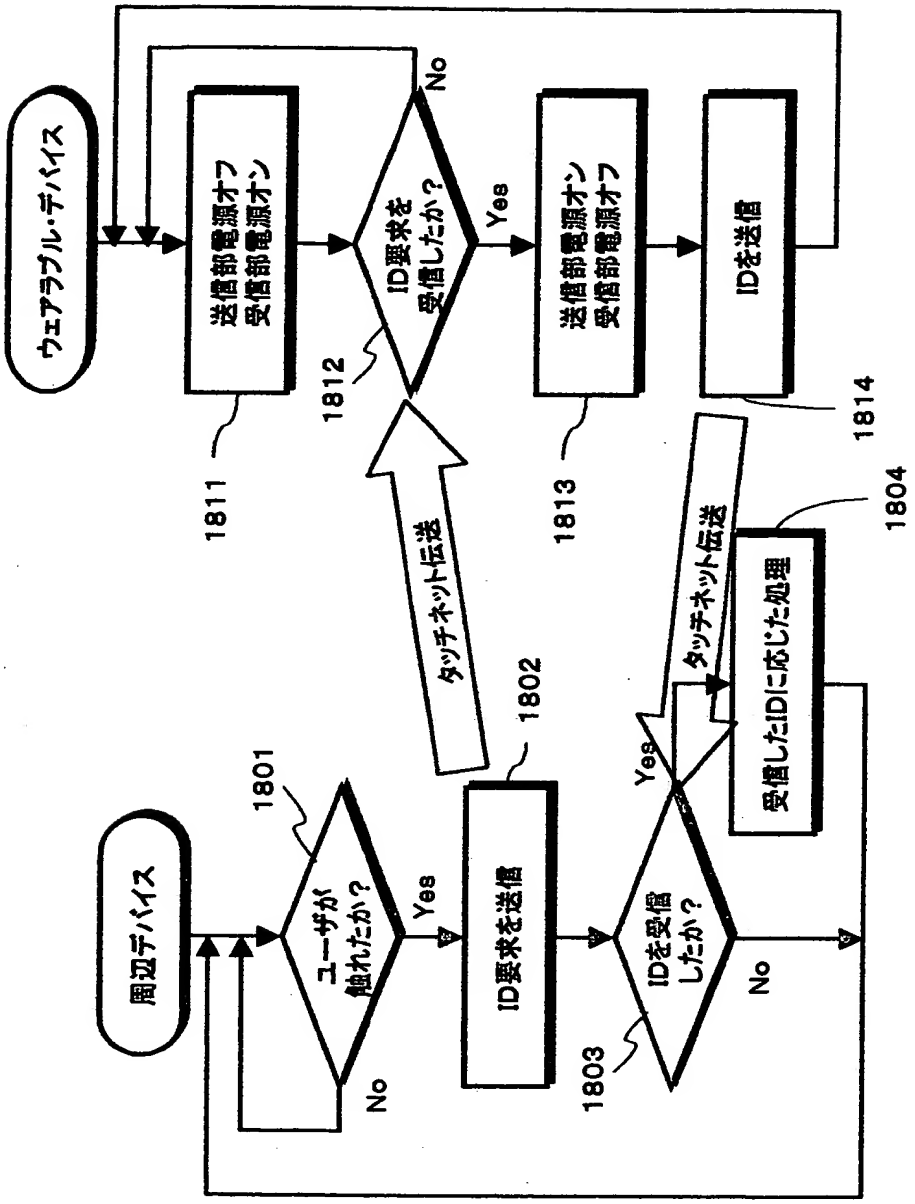
【図１６】



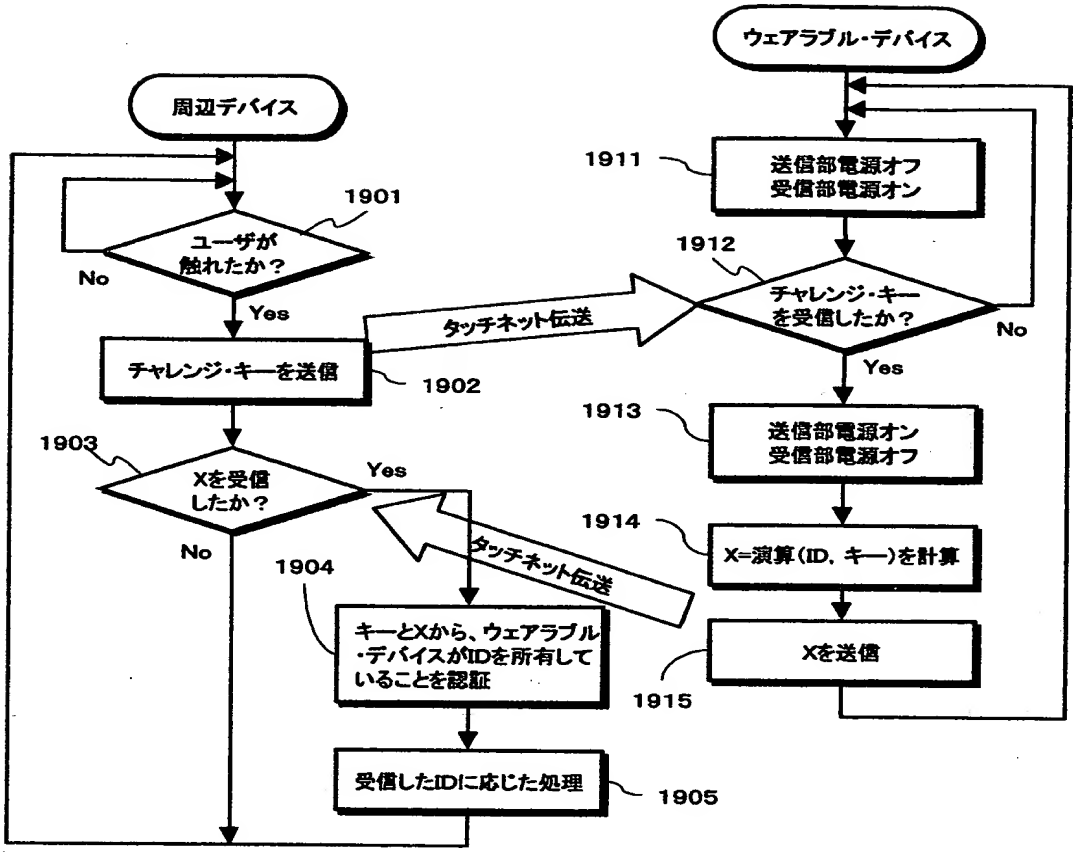
【図１７】


ウェアラブル・デバイス300
CPU 303
メモリ 304
タッチネット送信部 301
タッチネット受信部 302
電極
ユーザ
電極
タッチネット送信部 321
タッチネット受信部 322
周辺デバイス320
CPU 323
メモリ 324
駆動部 325
認証情報通信システム

【図１８】


ウェアラブル・デバイス
送信部電源オフ
受信部電源オン
ID要求を
受信したか？
No
Yes
送信部電源オン
受信部電源オフ
IDを送信
1811
1812
1813
1814
タッチネット伝送
タッチネット伝送
1804
受信したIDに応じた処理
1802
1801
周辺デバイス
ユーザが
触れたか？
Yes
ID要求を送信
IDを受信
したか？
No
No
Yes
1803

【図１９】


ウェアラブル・デバイス
周辺デバイス
1911
送信部電源オフ
受信部電源オン
1901
ユーザが
触れたか？
No
Yes
1912
チャレンジ・キー
を受信したか？
No
Yes
タッチネット伝送
チャレンジ・キーを送信
1902
1913
送信部電源オン
受信部電源オフ
1903
Xを受信
したか？
Yes
No
1914
X=演算(ID, キー)を計算
タッチネット伝送
1904
キーとXから、ウェアラブル
・デバイスがIDを所有して
いることを認証
Xを送信
1915
受信したIDに応じた処理
1905

【書類名】　　要約書

【要約】

【課題】　人体を介した通信により、提供サービスに応じた認証を効率的に実行する個人認証処理実行システムを提供する。

【解決手段】　ユーザが装着した携帯機器とサービス提供端末間での認証処理を、所定の接点にユーザの身体が触れるという物理的実感に応答して実行する。携帯機器に、ユーザ固有識別子と、提供サービスに応じて各ユーザ毎に生成されるユーザ可変識別子を格納し、サービス識別子に応じて、携帯端末でユーザ可変識別子に基づくサービス固有ユーザ識別データを生成して、これをサービス端末に送付し、サービス内容に応じた課金処理やユーザ管理を行う。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２０００－２５３３０５
受付番号	５００００１０７１１６２
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１２年　８月２９日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　000002185

【住所又は居所】　東京都品川区北品川６丁目７番３５号

【氏名又は名称】　ソニー株式会社

【代理人】　申請人

【識別番号】　100101801

【住所又は居所】　東京都中央区新富１－１－７　銀座ティーケイビル６階　澤田・宮田・山田特許事務所

【氏名又は名称】　山田　英治

【選任した代理人】

【識別番号】　100093241

【住所又は居所】　東京都中央区新富１－１－７　銀座ティーケイビル６階　澤田・宮田・山田特許事務所

【氏名又は名称】　宮田　正昭

【選任した代理人】

【識別番号】　100086531

【住所又は居所】　東京都中央区新富１－１－７　銀座ティーケイビル６階澤田・宮田・山田特許事務所

【氏名又は名称】　澤田　俊夫

次頁無

出願人履歴情報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社